Finextra | feedzai

Utilising AI to Prevent Financial Crime

A research paper from Finextra in association with Feedzai

Content

01
Foreword

Richard Harris
SVP, International Operations, Feedzai

Trust is the most important currency a bank has. Reputation in the marketplace and how consumers see a brand are more important than ever. But how do you maintain that when transactions are ever increasing in speed and complexity, the whole banking system is opening up, and financial criminals are becoming increasingly sophisticated?

One of the biggest trends in banking in the last few years has been the shift towards faster payments and open banking. Whether that's through specific policies like PSD2 in Europe, driven by regulation, or via customer demands for more open access to their financial accounts, we can be sure that this trend isn't going away. In fact, it's only speeding up as banks race to be leaders in this age of digital transformation.

At the same time, financial criminals are determined to get ahead in this technological game of cat and mouse. We see evidence of organised crime and money laundering employing Advanced Analytics AI and botnets, similar to what banks themselves are using. With the massive amounts of hacked data available for easy purchase on the dark web, and increased areas of susceptibility because of the shift toward open banking, many of these criminals are thriving like never before.

The University of Portsmouth's Centre for Counter Fraud Studies (CCFS) recently contributed to research that suggested "the UK economy could be boosted by £44bn annually if organisations step up efforts to tackle fraud and error, while globally, fraud is costing £3.24 trillion each year, a sum equal to the combined GDP of the UK and Italy."

So what do we do in a world where banks are competing to be omnichannel and open, criminals are ever more tech-savvy, and yet consumers are more likely than ever to drop a brand that they feel isn't securing their data or payments?

Machine Learning and AI has never been a silver bullet to detect fraud and financial crime, it's only ever been one part of a properly thought out strategy. However it's remarkable that in the rush to technology, we often still talk with companies who initially propose to build a risk management system in house, only to end up with a solution that – apart from being behind schedule over budget and less functional that envisaged – barely meets their most recent needs, and doesn't have the flexibility to cope with the fast pace of change the of financial crime across the market, or scale to the new channels where it'll be needed in the years to come.

What we need now is advanced machine learning, of course, but also an array of tools on top of that to deliver both the security and the customer experience that consumers demand. For example, our Feedzai Genome graphical link analysis tool gives analysts the ability to instantly map otherwise hard to detect illicit networks in a matter of seconds, while visually telling the story of how those networks interact and what they are up to. Then it gives those analysts the ability to instantly take action on the whole network.

Genome is just one example, aside from our core profiling capability and single view of a customer, that help keep the good guys in control, but more importantly, also helping to limit false positives and other issues that harm the customer experience of loyal consumers. It's also how we are helping banks

to get a fuller picture of their data, because in the end, a risk management solution should also be one that helps financial institutions to better understand and utilize their data.

So to go back to where we started, trust is the most important currency any bank has, and recent high profile cases across the financial industry show how that trust can be stripped away in a matter of days. With smart technology, combining machine learning with great tools and a flexible fast-moving platform, we're helping banks to do what they should do best – deliver great products.

02
Introduction

The convergence of open banking, data protection regulation, digitalisation of 05 services and advancement of technology and artificial intelligence has caused profound and prolific changes to the financial services industry. It has alsoopened new doors and fresh opportunity for fraudsters, who are equally taking advantage of new technologies and the reams of data that now exists in the banking ecosphere.

According to a 2018 Experian report survey, 37% of businesses are experiencing more fraud losses in the last twelve months than previously.

Keeping transactions secure as financial organisations move into a world of open banking is a race that gets faster by the launch of a new banking API. Risk management, cyber security and fraud strategists need to collaborate to stay ahead of the competition, while addressing the needs of the new digital customer, which includes the hefty task of protecting their data.

Questions about liability in multi-party transactions and ever-increasing systems and protocols abound, as businesses transform to an end-state not yet known. New attack vectors in transactions and account opening come to the fore on a daily basis. How can banks utilise Machine Learning (ML) and AI in the fight against fraud in this real-time and fully digital marketplace?

With the emergence of open source technology, is there scope for data sharing to arm organisations with real-time information and anomaly detection? Could business functions communicate better internally to support the fight against fraud?

This research paper by Finextra, in association with Feedzai, gathers the views of several senior data science and fraud experts from across the financial services industry on how to tackle fraud with AI as open banking and digitalisation continue to evolve.

03
Types of attack on the increase

When it comes to protecting the customer, a multi-pronged approach is necessary, and it is paramount to stay abreast of fluctuations in trends and tactics that fraudsters employ. Banks need to know where the vulnerabilities sit, and this can change rapidly.

The vulnerability around identity is stressed by Ghela Boskovich, Founder, FemTechGlobal, too, who opines "the point of most exposure is the third-party providers, due to the exchange of Personally Identifiable Data (PII)".

According to Paul Schooley, Chief Operating Officer, Cashplus, account opening is under more pressure at the moment than transactions in terms of fraud attacks and losses as a result, because it relates to impersonation and stolen IDs– the downward stream fallout of other organisations having data breaches.

"Our credit products aren't necessarily having the same type of challenges, but on our current account side, we continuously modify and update our overall framework." he says.

"Transaction fraud we can pretty much identify and manage with our algorithms, and exposure there is limited– there haven't been any surprises," says Schooley.

Phishing attacks, however, are on the rise, he adds, "Cashplus has reached the size where kits for producing dummy phishing sites can be bought by organised criminals. So developing algorithms to help counter that, by better identifying legitimate users vs 'black hats' has also been a focus in the last six months or so."

Social engineering continues to be a big vulnerability that the industry must work with each other to educate consumers and businesses on. "The 'Oh, you have a problem with your WiFi account, call us up and let us take over your computer to fix,' type of calls to individuals continues to be a problem," Schooley explains. "Social engineering type of fraud opens the protection question out

to user awareness. It falls to the industry to understand how consumers can be better educated on the dangers of these types of scams, he maintains. He references the Take Five initiative, a national awareness campaign led by FFA UK (part of UK Finance and backed by the government. "It remains a challenge to ensure the message is getting through to the right people, and at the right speed," Schooley concludes.

A fraud expert at a top Irish bank said "What we're seeing is the customer being targeted, rather than the bank per se. APP-type scams, invoice redirections, where our customers are the weak link in the security infrastructure. The bank's IT security perimeter is very robust, you can see literally thousands of malware and similar automated attacks every day that are repelled, but through social engineering and all the different types of techniques, the criminals then go after the customer."

He said most fraud losses are suffered on credit cards, about 90%, as a result of compromised information harvested from external data breaches mostly. Money muling is a problem across the industry as a whole, where customers knowingly or unknowingly surrender account details to third party fraudsters. Younger customers in particular, are vulnerable to being targeted to act as money mules. Electronically-enabled fraud is up about 60% from two years ago, about 25% year-on-year.

"Absolutely more could be done to share information. In Ireland I describe fighting financial crime as like having one arm tied behind your back. For data protection reasons I cannot share details of an account I deem a risk with another bank, which is different to the UK. There are industry proposals for a change to the current law to explicitly permit an appropriate exchange of fraud information between the banks. The penalties for breach of GDPR are notionally bigger than breaches of AML legislation. We share fraud intelligence with the Gardaí (Irish police), who, by virtue of operating a single unified policing authority, play a key role in the overall financial crime response in Ireland. There is a strong working relationship between the different financial crime teams within the main Irish banks with the Gardaí through the Banking and Payments Federation of Ireland, which enables proactive responses to observed fraud and AML threats."

On phishing attacks, Boskovich says the mobile channel is the prime target. Seeing as banking services are converging ever-more on the mobile channel, however, this becomes an increasing challenge. And to counter this, a secure dev ops environment is key, she says.

"Studies show time and time again that users are three times more likely to fall for phishing attacks via a mobile device than they are through other channels. Overlay attacks, phishing attacks and mobile app threats, this all rolls back to having a secure dev op environment, and a mobile application shielding framework."

Human behaviour needs to be factored in as well, of course. While fraud and phishing fall to the dev op environment to protect, the dev op environment cannot necessarily mitigate human behaviour.

Richard Dupree, Senior Vice President, Group Operational Risk Manager, Bank of the West, further emphasises identity and account-based attacks over transaction fraud as being most under attack and calls out business email compromise– sometimes called CEO impersonation, as having increased over the past few years. This is where fraudsters impersonate trusted senior corporate executives or business suppliers who regularly request money transfer and payments, he explains. Unsuspecting employees process the requests, usually in the form of a wire transfer, and send the funds to a fraudulent beneficiary. The fraudsters on the receiving end usually withdraw or move the money before the fraud is identified.

"This type of fraud is difficult for risk teams to manage as it represents a breakdown in the customer's control environment and not that of the financial institution (FI). It would behoove FIs to offer a wire or payment product with controls, such as user authentication and dual approvals, embedded in the system so as to dissuade manual outgoing wire requests by customers," Dupree adds.

Dupree also mentions Account Takeover Fraud (ATO), whereby fraudsters obtain access to an account through various techniques such as social engineering, vishing (differing from phishing in its use of voice) and malware. They then pose as the account owner to change contact information on the account, move money, withdraw funds, and possibly use the stolen information to access other accounts, as most people use similar or the same passwords across multiple platforms.

Types of fraud are changing all the time, in the same way that financial organisations adapt continually to deploy new forms of technology, so fraudsters constantly adapt their approach to exploit new vulnerabilities or leverage new technology to further their cause. Can organisations keep up with the pace of change? Martin de Vries, Information Security Officer, Rabobank says yes, although the speed of change will always be a key challenge.

"From a knowledge perspective, organisations can keep up. Adapting the business is a slower process. Banks and partners need more time to adapt or respond to new threats. I think that will always be the thing. They might be able to identify threats sooner, but in the end those technologies need to be implemented in the response, and that kind of stuff takes time."

04
Utilising AI for protection against increased fraud vulnerability

What are organisations doing then to counter the evolving and persistent threat of fraud– how are they leveraging the emerging suite of tools that AI provides to adapt and prevent attacks, keeping data, accounts and transactions secure?

Reducing false positives is an obvious use case for AI, simply because the numbers are so high. Abhijit Akerkar, Head of Applied Sciences – Business Integration, Lloyds Banking Group, says, "Over 90% of the financial crime alerts are false positives for many banks." Utilising AI will definitely help but only to a certain point because criminals operate across borders and banks whereas "banks see only a fragment of the picture".

Furthermore, Ghela Boskovich points out that banks can "use AI to look at the set-up of the transaction itself, the onboarding of customer accounts– scanning data on the KYC side, and anomalies individual records." Essentially, anything that establishes identity.

So this is bringing AI in at the outset, to cover the identity piece. Every single payment is required to have authentication. Sanctions, pathways, ensuring records are updated real time. "So if you've got AI applied to the identity component early on, this allows us to make a very valid assumption that going forward, the authentication component is going to be valid, and that feeds into the assessment of whether or not it's a fraudulent transaction further down the value chain," Boskovich asserts, which would reduce the number of false positives, and the exposure to fraud, she says.

When asked whether organisations were already there with this concept of employing AI at that identity point, "No," came the emphatic answer. Bank of the West's Richard Dupree says organisations need to deploy machine learning to model account behaviour and detect anomalies in real time, adding, "Rule-based approaches to managing fraud aren't nimble enough and create too many false positives, which adversely impacts the customer experience. Multi- factor

authentication should be used when users sign in from a new device and SMS/email alerts when account changes get processed."

For SIM Swap fraud, Cashplus has put in algorithms based on patterns, to hold some payments longer and go through enhanced verification. And the protocol allowing people to redirect one-time passwords over mobile phones has caused them to adopt bio– and token-related methods in the next 12 months. What is fast becoming clear, is that a carefully considered and bespoke approach is required for combating each different type of fraud.

"For each type of fraud, a different strategy, different algorithm and different process is needed. We have to step back and understand the attack vector they're using– what kind of weakness point they are actually exploiting," Cashplus' Schooley explains.

"In some situations, you cannot mitigate, you just have to ensure you have improved identification through certified algorithms, that ensure manual review and verification. Additional friction is key, for example with SIM Swap, a SIM is something you have (possession) so let's augment it by something you know (knowledge), which the SIM Swappers won't have."

"Account opening is under more pressure at the moment than transactions in terms of fraud attacks and losses, because it relates to impersonation and stolen IDs– the downward stream fallout of other organisations having data breaches."

Paul Schooley, Chief Operating Officer, Cashplus

05

Data and AI capability

Data science supports fraud and financial crime programmes in organisations in different ways: transaction monitoring, customer risk and settlement.

“Data science, in combination with artificial intelligence reduces the rate of false positives,” says Angel Serrano, Head of Data Science, Santander.

“We don’t use automation on data science, we use data science to help automation and analysis of huge data sets from the data lake built a few years ago, for example, manual classification of customer requests, recorded in 100 different categories. We created a robotic solution that automates the process. It takes the text and applies the data science model, which defines the class that the request should be, then uploads the output on what it should be. So, we’re using data science to automate process by embedding the model into an RPA solution.”

According to Ghela Boskovich, patterns are easy to detect in structured transaction data, of which banks have plenty. However, they also have copious amounts of unstructured data. “What actually matters is not necessarilythe algorithms but the data science that structures things before it gets into the algorithm.” Pattern recognition on structured data can produce a setof anomalies that are easy to scan for, and that can continuously scan the unstructured data.

Serrano maintains the main benefit of AI is in reducing the number of false positives, and in helping target and identify fraudulent transactions more efficiently. “By itself a transaction says a lot, but if we enrich with existing data we have about the customer or about, for example, the account where it was originated or information about the originator, that we have from other sources, we have way more rich data, and then that knowledge is way more powerful.”

And this distinguishes AI’s capability beyond traditional analytics– for predicting future outcomes or patterns.

"At the moment the value chain is filled in by multi-party systems. It still isn't 100% clear who carries the ultimate responsibility on the cyber security side when it comes down to a transaction that is initiated through a third-party app. We have a multi-level cybersecurity system the moment you talk about an open banking-based proposition."

Paul Schooley, Chief Operating Officer, Cashplus

Richard Dupree agrees with this sentiment, saying, "Data can be leveraged to create a profile or model of the customer's typical activity to be used as abaseline when a typical transaction activity takes place. Counter measures can then be applied instantaneously and with better precision. Data is being used by criminals to commit financial crime. It needs to be used better by banks to fight financial crime."

The challenge of managing data in a digital world, however, as articulated by Serrano, is having the requisite data to feed into the models. "To create an advanced model, we typically request at least two years of data, and that data has to be labelled, meaning we need to know whether it got flagged and sent to the authorities or not or passed to the next line."

Akerkar reinforces this issue, saying that any new regulation poses a typical challenge for AI systems – lack of training data. The AI systems will need sufficient numbers of transactions in the new regulatory regime to train themselves well enough to spot anomalies and fraud patterns. Generally, one to two years of data is considered good enough. So the question is how to prevent fraud in the meantime.

"Proactive transaction monitoring," ascertains Akerkar. "To stay ahead of the curve, banks will need to build the capability to recognise patterns in huge amounts of dispersed data using machine learning and in subsequent organisational decision-making. Banks will need experts who would make sense of those patterns and develop rules to prevent fraud. Generating synthetic data to simulate potential cases is an alternative that banks can explore to train the AI systems. More importantly, banks will need to build flexible systems that can adapt and evolve as the unknowns evolve. We yet don't know how customers will take up open banking and how criminals will react," Akerkar says.

The Irish banks' fraud expert says AI will come into its own in sophisticated transaction monitoring, "using smart rules to automatically close some alerts, hibernate others, and bring others up for immediate review– to segment them".

06

Visualisation is power

The art of visualisation comes into play when trying to make sense of the sheer amounts of data banks now have at their fingertips. How important are visualisation techniques in defining a fraud strategy?

Says Serrano, “It’s very important in the early stages, when we build a model we work with the financial crime team in order to identify what are the key features they need to define a risky transaction– to identify the right characteristics of the model. Then we work to present visually– perhaps 3D, how different clusters of transactions behave. What the first line usually cares about is the number of alerts that they have to review.”

Lloyds’ Abhijit Akerkar credits visualisation methods used by the International Consortium of Investigative Journalists (ICIJ) in the unfolding of the Panama Papers scandal. “For developing a top level view, helping humans make decisions, making sense of the zillions of data points in front of them.. [visualisation] definitely plays an important role and banks are already using it.”

Visualisation allows databases to be graphed, quick associations to be made and a more efficient processing of those associations. The question is what level of investment in these tools makes business sense.

De Vries counts visualisation as “more and more important”, so much more efficient than analysing raw data or just looking at the figures.

07

Open banking open doors

The collecting and sharing of data, the question of liability and varied business function Data Strategie

Without doubt there is concern among financial organisations about new vulnerabilities that open banking will bring about in terms of fraud and risk. The concept of capturing and sharing information is multi-faceted. There is the question of keeping a transaction secure when third parties become part of the value chain and there is the capturing of data to inform fraud strategies, and the use of AI and emerging technology to track behaviour and identify anomalies, and hence, so-called bad actors. A large part of this conversation centres around where liability sits when there is a proliferation of parties and providers who may now be part of a transaction.

Marco Bosma, Senior Vice President, Fintech and Innovation, Rabobank, raises a valid point around this, “At the moment the value chain is filled in by multi- party systems. It still isn’t 100% clear who carries the ultimate responsibilityon the cyber security side when it comes down to a transaction that is initiated through a third-party app. Clearly the identity check and everything is with the fintech third party– they will have had to prove this in order to get the licence– so we have a multi-level cybersecurity system the moment you talk about an open banking-based proposition.”

With data sharing, first it has to be anonymised. Bosma talks of propositions in this space and how it falls to the system integrators to provide the secure APIs. “We look at it as a security layer that needs to be embedded into the API, and the fintech party has the security layer in the sign-in part and they share that information across the API layer, hence the enormous call for standardisation, because otherwise every implementation becomes very bespoke and cumbersome,” Bosma adds.

Abhijit Akerkar has a similar take on the impact of open banking on fraud. “To detect anomalous behaviour, banks need to interact with customers to recognise the ‘normal’ behaviour. But with open banking, customers’ interaction with banks might reduce as they allow third parties to interact on their behalf. This reduction in customer interaction could reduce the ability of banks to

detect the anomalous behaviour. As banks open up APIs to third parties, and once a customer has allowed third parties to do transactions on their behalf, what essentially happens is that fraudsters get a bigger space to operate in."

"As an industry, we have moved too fast with open banking, and with the desire to move everything faster, you are effectively abandoning a lot of the controls you need to put in place, so we need to try and rein in that horse," says the Irish bank's fraud expert.

Paul Schooley expresses financial firms' valid fears around data collection,in light of current regulatory updates. "Collecting data on a person from an authentication upfront I think definitely has a lot of interesting applications, and can be used to effectively mitigate a lot of account opening issues that you have around the fraud space." But this needs to be carefully considered, he states, as some take a cynical view on this kind of blanket data capture. However, in terms of capturing data on your customers as they interact on your platform, well that's absolutely fair game. As long as policy statements around privacy are up-to-date, of course.

Within the obligations of GDPR, collect as much data as you can, wherever you can, from whatever device you can, from whatever interaction you can. And then determine how to translate that data into meaningful decisioning points that protect the customer." Most interestingly, he adds, "even if you don't have the capacity to turn it into a refined decisioning tool at this point, just capture it and archive it, or store it. Storage is cheap," Schooley says.

"Money launderers don't launder through one bank but different banks and different countries. Are countries and banks sharing the information with each other? Not to the extent required. Unless and until countries and banks step up their information-sharing partnerships on financial crime, money launderers will continue to have the advantage."

Abhijit Akerkar, Head of Applied Sciences, Lloyds Banking Group

The importance of information sharing is illustrated in a compelling way by Abhijit Akerkar, at the same time putting another slant on the vulnerability open banking brings about.

Money laundering– as discussed, nothing in itself to do with open banking, but an area with very high false positive ratios– in the region of 90% on average for many banks. “Money launderers don’t launder through one bank but different banks and different countries. Are countries and banks sharing the information with each other? Not to the extent required. Unless and until countries and banks step up their information-sharing partnerships on financial crime, money launderers will continue to have the advantage.”

Add to this of course banks’ inherent reticence in sharing info on vulnerabilities and the challenge is intensified.

The Irish bank’s fraud expert says bodies should come together more, rather than spending billions of pounds on “trawling exercises”, mining transactional behaviour and throwing away 99% of the outputs, rather than intelligence-led investigations. In Ireland, the police are central to the sharing of information on fraud between financial organisations.

Internally, however, banks are beginning to break siloes between cyber security, risk and fraud teams, in terms of sharing data, both the Irish bank fraud expert, and Akerkar affirm.

Martin de Vries, of Rabobank, further asserts there is sufficient communication and sharing of information between fraud, risk and cybersecurity, be it regarding a data breach or fraud, or new technology on the horizon that could potentially be deployed by fraudsters.

Richard Dupree, however, says that results aren’t generally shared outside of the function. “Reports are generated for management and governing bodies, but the data itself goes no further. Action may be taken as a result of the data, however, such as adding controls within the call centre or revisiting wire controls. Fraud data could be utilised more meaningfully within the FI such as to inform an emerging risk function, risk identification efforts or the efficacy of the control environment. Anti-fraud efforts may catch fraudulent activity before a loss occurs but the underlying control environment should be reviewed, taking into account the attempted fraud activity as there may be an opportunity to tighten underlying process controls.”

Given a recently published statistic that 90% of all information ever has been created in the last two years, what are the most important aspects of managing and leveraging that data in the best way possible?

Cashplus' Schooley: "I think there's going to be a push forward for greater data accessibility but I think that's going to be more based on the individual's opt-in selection at the point of interaction, as opposed to companies on the unilaterally deciding to re-use or share existing customer data internally."

Ghela Boskovich says the trusted data sharing infrastructure exists already, in a manner of speaking, but the payment ecosystem is currently overly complicated, with many unnecessary steps. "When we start to implement tokenisation on a mass scale, that allows us to fully encrypt the data, and not have it exposed or sitting outside the institution and its networks, this will reduce some of the haziness around liability. Those that encrypt and send out the data are liable."

Boskovich says this direct linkage will cut out extraneous players "that don't actually serve purpose other than they have rails" and will enable players to issue, process, remit and settle between institutions: ergo, fewer points of exposure.

Tokens, she adds, are best used for structured data fields, but they don't allow for unstructured data, so they are limited in that sense. Encryption (specifically homomorphic encryption) allows both structured fields and unstructured data.

Unstructured data allow us to see patterns beyond our limited reference points. Tokens are not embellished with any unstructured data that allows us additional insight. It is all mapped to a field, so pattern detection is limited," Boskovich says.

"As an industry, we have moved too fast with open banking, and with the desire to move everything faster, you are effectively abandoning a lot of the controls you need to put in place, so we need to try and rein in that horse."

Fraud Executive, Top Tier Irish Bank

08
Key challenges in Fraud and Data Management

Rabobank's Martin de Vries says the toughest problem is the amount of systems and IT that needs to be addressed, with the number of applications growing and the number of infrastructures growing as well with the cloud. Knowing, at every single point, where your vulnerabilities are, is crucially important.

"Manual assessments suddenly just don't cut it anymore and you need to look for tooling that helps in identifying weaknesses, vulnerabilities, risks– and that's the biggest challenge," he says. De Vries feels the proliferation of applications and infrastructures is only going to increase in the coming years.

"Expert knowledge, to ask the right questions and judge whether you have the right tools to run the data through to check for correlation," says De Vries. Interestingly, he adds, "most of the time the end results are not relevant and very few times do you get real insights. In the end it comes down to someone who knows their subjects, the business and the processes, and is actually able to ask the right questions, which translates to having the right answers."

This leads to the question as to whether AI or machine learning models will ever be intelligent or sophisticated enough to be that expert eye, to recognise and interpret patterns that emerge and suggest rules to safeguard against a potential threat?

Machine learning systems could be built to have the auto-rule generation capability. However, the role of humans will not disappear," Lloyds' Akerkar says. "It's more like humans getting super human powers with the help of AI to better predict and prevent fraud.

Martin de Vries shares the same view: "Personally, I would say no. I doubt there will ever be a situation where we will say, 'Hey, this is good enough, I don't have to do anything else.'"

"Anti-fraud efforts may catch fraudulent activity before a loss occurs but the underlying control environment should be reviewed taking into account the attempted fraud activity as there may be an opportunity to tighten underlying process controls."

Richard Dupree, Senior Vice President Group Operational Risk, Bank of the West

Data quality is another key challenge. As Richard Dupree says, for larger, 19 established FIs, not everything is digital, so managing risk usually requires toggling between automated processes and manual ones. Hence, data quality has become more of an issue with digitisation, as inferior data impacts the entire supply chain now as opposed to when processes were manual and disjointed.

"Quality data is critical to success of digital initiatives like ML and AI where one break in the link can jeopardise the entire solution. Data quality and governance should be a high priority at any FI with the appropriate resources, controls and attention allocated to its oversight," Dupree says.

09

AI to enchance – But should you build or buy?

Many FIs have implemented AI and ML models to automate rules-based processes to fight fraud, but not all have transitioned completely. It is becoming clear that a very tailored approach for each type of fraud is necessary– this is time-consuming and costly, and in large part unavoidable. Would a partnership strategy help here? It differs greatly from organisation to organisation.

Cashplus' Schooley, "The key thing to remember is that AI algorithms really need to be tailored specifically for that use case and indeed client in question. Something to bear in mind when considering partnerships or buying off-the- shelf solutions. Algorithms need to be customised to an organisation's own population "to get better separation", Schooley says.

"I don't see a turnkey model or algorithm solution really being viable. I think each one has to be bespoke to that individual, that business, and that business model," he continues.

"Partnership is definitely the best strategy– to build those solutions in-house is a monumental waste of time and money," says Ghela Boskovich, referring to identity, KYC and compliance tools specifically. This keeps dev op teams focused on what they should be doing, which is developing other solutions not on the market, she adds.

"Partnerships also mean quicker deploymen– in the cloud or private cloud– having the flexibility to put in a sandbox to run tests before you put something into production, and making it easier to upgrade if you move to a different solution provider. And you have a proper API structure in-house, and can find the datasets more easily with an API framework in place."

Paul Schooley says a partnership strategy completely depends on the size and scale of the organisations; says Richard Dupree, most banks have in-house fraud expertise but could benefit from technology solutions experts in the space.

10 Future outlook conclusion

Back-office functions, in retail banking, will be transformed by Robotic Process Automation (RPA), for example the handling of dispute forms will be automated, and the human element will simply be in reviewing the quality of the automation.

In terms of machine learning, the major arbitrator will be the regulator, Schooley says, "and where the regulator mandates an understandable decisioning action, and where they are open to some fuzzy logic that protects the customer better but might not be 100% explainable."

Currently, for managing fraud risk, we take the latter approach which results

in not explaining 100% how the algorithm is operating, Schooley adds. "As long as it's showing the success of the algorithm to protect your customers as well as the banking system." He points out that in understanding why a customer was declined, for underwriting of credit bills, a regulator will always want to see point blank what the reasoning was, "which, with machine learning techniques, is very difficult to do."

Bank of the West's Dupree says, "In particular, AI will empower risk managers to take a more proactive and forward-looking view of their risks by focusing on analytics across the organisation, processes and control environments rather than having to manage risks through a list of siloed processes."

One thing is clear, with the sheer amounts of data financial organisations are dealing with, traditional processes no longer make the grade. AI is already needed in a merely operational capacity. Machine learning models can be developed and deployed to understand better customer behaviour, and the most coherent strategies would have ML and AI capability built in from the outset of a customer journey, to strengthen the identity piece. The greatest vulnerabilities lie around the identity of the customer, be it in account opening fraud, account takeover fraud, imposter fraud, etc.

As the Irish bank's fraud expert says, "banking is moving so fast, the fraud environment is really struggling to keep pace with it. The card guys are using adaptive technology to screen a payment in a billionth of a second but we need to get to that level with payment processing as well. There's a lot of monitoring on outgoing payments, I don't think we do as much on incoming payments."

In terms of the fight against transaction fraud, tokenisaton is touted as being a key differentiator. Whether banks and other financial organisations move towards a more collaborative approach with regard to the information they hold on fraud is yet to be seen; certainly, this is incongruous with the competitive nature of the market in which they operate, however, twenty years ago, who would have thought that third party payment providers could be playing such a proactive role in the movement of monies as they will do from here on in.

Artificial intelligence is there to enhance the ability to process and leverage data– it is a sophisticated toolkit, that ultimately must be driven by the goals of the business in question. Human supervision is not expected to be surpassed or usurped by intelligent technology. And human designers and developers would do well to ensure they factor this in at this stage of the game.

One thing is clear, with the sheer amounts of data financial organisations are dealing with, traditional processes no longer make the grade. Machine learning models can be developed and deployed to understand better customer behaviour, and the most coherent strategies would have ML and AI capability built in from the outset of a customer journey, to strengthen the identity piece. The greatest vulnerabilities lie around the identity of the customer, be it in account opening fraud, account takeover fraud, imposter fraud, etc.

11 About

Finextra

This report is published by Finextra Research Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participates in posting their opinions and comments on the evolution of fintech. In addition, community members contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra, contact contact@finextra.co or call +44 (0)20 3100 3670

feedzai

Feedzai is the market leader in fighting fraud with AI. We're coding the future of commerce with today's most advanced risk management platform powered by big data and machine learning. Founded and developed by data scientists and aerospace engineers, Feedzai has one mission: to make banking and commerce safe. The world's largest banks, processors, and retailers use Feedzai's fraud prevention and anti-money laundering products to manage risk, while improving customer experience.

Visit feedzai.com and follow on social media for more information and the latest company news.

Finextra Research Ltd
1 Gresham Street London
EC2V 7BX United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any

means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without prior permission in writing from the publisher.

© Finextra Research Ltd 2020

Feedzai is a registered trademark of Feedzai, Inc.