NAME:AMIT DUTTA
ID:1810011010

STREAM:BCS4A

SUBJECT:-ARTIFICIAL INTELLIGENCE

TOPIC :- AI for fighting Financial Crime

Fighting Financial Crimes with Artificial Intelligence

Fighting financial crime with AI

The latest research shows that an epidemic of financial crime is costing society $4.2 trillion globally. As new digital channels emerge for financial transactions, financial crime just keeps growing worse. Whole communities of fraudsters and criminals are continuously innovating new ways to steal, and they collaborate with one another and sell their tactics and techniques in a seemingly insatiable, world- wide black market. Legacy practices and traditional rules engines can't keep up. We need new approaches.

Artificial Intelligence (AI) offers a way forward. AI techniques, although new, have already been proven to thwart a variety of financial crimes. This report provides the following.

- Insights from executives who share their experiences in apply- ing AI in the fight against financial crimes. Unlike many strategic technology areas in which methods and outcomes are closely guarded secrets to protect competitive differentiation, this report spreads ideas and best practices from real-world implementations.
- Visibility into successful outcomes, and thought leadership on challenges, countermeasures, and the problems that still need to be solved to turn the tide in the fight against financial crimes.

AI conjures different reactions ranging from scepticism to irrational exuberance, and this report aspires to leave you with a practical understanding of the exciting current capabilities as well as current limitations of applying AI in the fight against financial crimes.

Financial Crime Continues to Increase

Recent research finds that global financial crime is massive in scale and accelerating in pace. One study put the current global cost at $4.2 trillion. Another estimated that the typical organization loses as much as 5% of revenue to fraud each year. And every $1 of crime costs businesses between $2.48 and $2.82 in total—that's about two and a half times the direct loss itself. Extra costs include regulatory fines for noncompliance, operational expenses for dealing with the aftermath of crimes, notifying and compensating the victims, and the financial fallout from reputational hits. Unfortunately, financial crime is only accelerating. In 2017, two-thirds of businesses experienced financial criminal activity first hand sharp 58% increase since 2016. In a recent interview with Bank Info Security, Daniel Cohen, head of RSA's fraud and risk intelligence product suite, said this:

> *If we are predicting that transaction volumes are going to grow, then, obviously, fraud cases, and I'm talking in real numbers, are also going to grow significantly. And then there's the whole operational question of, 'How do we manage and mitigate the fraud that the bank is suffering?*'

Different Types of Financial Crime

Financial crime encompasses a varied and wide collection of illegal activities. For the purposes of this report, we divide them into three categories: fraud, money laundering, and cybercrime.

Fraud

Fraud schemes are sophisticated and change from day to day. Auto- mated systems as well as human fraud analysts pour over data and documents and review suspicious activity reporting (SAR) logs to determine which transactions are genuine and which are fraudulent. Here are a few of the most common fraud practices:

CREDIT CARD FRAUD

> *Linked to the rise in online commerce, the most common kind of credit card fraud is called card not present (CNP) fraud. CNP fraud occurs when a fraudster purchases a product or service online and is not obliged to present the card or provide a PIN or signature. CNP fraud can also be a type of identity fraud in which a fraudster takes over the digital identity of a victim and opens credit card accounts or runs up bills in the victim's name. Although many experts attribute the increase in CNP fraud to the implementation of Europay, MasterCard, and Visa (EMV) chip technology, there's also the fact that online commerce is booming, and fraud prevention tools have not caught up. Financial institutions unfortunately bear responsibility for most of the money lost as a result of CNP fraud. The Nilsson Report in October 2016 showed that card issuers paid a 72% share of fraudulent loses , with merchants and ATM acquirers paying the other 28%.*

Synthetic identity fraud

> Synthetic identity fraud is an increasingly common type of fraud. In this case, the fraudster creates and establishes credit using a false persona, which is often a sophisticated blend of faked and real personal details; for instance, using a fake name along with a real social security number, such as that of a child, to lend the persona credibility. Pupating the persona, the fraudster patiently mimics legitimate financial behaviour staking out loans, withdrawing cash advances, and running up bills, but always acting properly and paying on time to establish the credit-worthiness of the synthetic persona and grow the line of credit. Then, they perform what is called a "bust out" in which they max out the cards, max out the cash advances, default on all loans, and disappear. This type of fraud is very difficult to catch in advance because the fraudsters do nothing wrong until , all at once, during the bust out, they do everything wrong

ACCOUNT TAKEOVER

Account takeover fraud is a form of identity theft in which a third party gains access to unique details of a user's online accounts. By posing as the real customer, fraudsters change account passwords and phone numbers, buy goods and services, withdraw funds, and use the stolen information to access other accounts of the victim. Exact figures are difficult to esti- mate, but one study from 2017 concluded that account takeover fraud had increased year-over-year by more than 45% and was costing merchants more than $1 billion every month.

MONEY LAUNDERING

Money laundering is the process by which criminals trick authorities into making it seem like the monetary proceeds of illegal activities came from legitimate economic activities. For instance, one typical money-laundering scheme involves using criminally acquired money to purchase subjectively valued items such as real estate, art, or antiques. Or a fraudster can buy chips at a casino with illegally acquired money, exchange the chips for cash, and claim that the actually ill-gotten monies were merely legitimate gambling winnings. By obscuring the identities of transaction partners, Bitcoin and other cryptocurrencies are also becoming a problem for financial institutions.

Benefits of AI-Based Models to Fight Financial Crime

Financial services firms are finding that AI-based models deliver measurable value, even at this fairly early stage of deployment. Here are some of those benefits:

AI AUTOMATES RULES CREATION

In a traditional rules-based TMS, a human must identify rules that will cleanly distinguish criminal from legitimate transactions and then program the rules into the system. By contrast, an AI-powered system can be thought of as an automated rules making machine. Instead of requiring a human to look at, analyse, and identify criminal patterns, rules emerge directly from the data through the process of training the AI model.

AI CAN CATCH CRIMES TRADITIONAL RULES CAN'T

Machine-made rules, derived from massive quantities of com- plex, nonlinear, and time-delayed data, can be subtler and more accurate than those that a human can discover or articulate. AI makes "hiding in the noise" much more difficult.

AI DECREASES FALSE POSITIVES

Not only do AI models improve the accuracy with which crimes are detected, but AI approaches can simultaneously reduce the flood of false-positives that are so costly to internal security operations and to the institution's reputation. Traditional machine learning (ML) techniques are almost universally plagued by a trade-off between false-positives and false negatives: With AI, it's now possible to use data to improve both problems at the same time.

AI IS AGILE AND ADAPTIVE

AI's agility and its ability to help you stay current with everchanging threats is one of the biggest advantages of AI. That's because AI can adapt on the fly to changing threat behaviours. And when an AI system sees something it hasn't seen before, it can be programmed to issue an alert and to say, in effect, "this is something I've not experienced previously, therefore I need to have a human review it." The more the system is used, the more it learns, and the better it performs—unlike a rules-based sys tem, which simply reapplies the same rules over and over again. All results can then be fed back into the TMS based upon evidence-based investigation rather than guesswork.

AI ACCELERATES HUMAN TEAMS

AI-based models can automate many of the currently manual steps involved in a transaction investigation so that the complete vetting of even complex transactions can be done in minutes rather than the half hour to an hour that it can take using traditional rules-based systems.

AI IS OBJECTIVE

AI models make “adaptive workflows” consistent and disciplined, and—very important—clearly document them. You can make investigations specific and tailored to each alert, case type, business unit, asset class, or behaviour type, while at the same time reducing the amount of analyst subjectivity and increasing the reliability and auditability of the investigation.

AI INCREASES ANALYST VALUE ADD

With detection accuracy up and false-positives down, analysts no longer need to process high numbers of mostly false-positive alerts. Instead, they can follow only those leads more likely to actually be fraudulent or otherwise illegitimate and perform only the higher-level manual analyses that at this point are still beyond the capabilities of AI.

AI CUTS COSTS WITHOUT RISKING YOUR EXISTING INVESTMENTS

You will be able to reduce the size of your investigative units, cutting costs by as much as 50%—but also realizing 50% greater efficiencies with the TMS technologies and processes you already have in place. AI doesn’t replace existing systems; rather, it integrates with them: AI supplements the strengths of the transaction monitoring and case-management systems and makes up for their weaknesses.

AI ANTICIPATES FUTURE REGULATION

In late 2018, the US Treasury Department’s AML unit and federal banking regulators issued a statement encouraging financial institutions to use AI as part of their approaches to fighting financial crime. Although neither providing safe harbour to innovative firms that use AI nor describing new compliance protocols, the move by US regulators strongly suggests that they are moving toward a world that welcomes if not mandates sophisticated new anticrime approaches that make use of AI.

Challenges of Deploying AI Models when Fighting Financial Crime

Yes, there are many advantages to using AI to fight financial crime, but there are also challenges. AI is not a panacea against financial crime. There are some significant challenges—challenges that most financial firms need expert help to overcome—to deploying AI successfully.

AI MODELS CAN’T JUST BE HANDED OVER TO IT

Historically, the data science team created a machine learning model or analytics algorithm. The model would then be handed over to an IT team, which would implement it and integrate it in production systems. Because of this handoff, there would typically be a six month gap between developing, testing, and tuning the analytical model on archival data and actually deploying it so that the model could make operational decisions on live data. Two totally different organizations would be involved.

MODEL EXPLAIN ABILITY CAN BE DIFFICULT

Another challenge is explain ability. Many regulations require that your decision-making processes be transparent. “You may build a sophisticated, advanced machine learning way of detecting money launderers, but if you can’t explain it to a regulator, and if you can’t ensure that it aligns with key aspects of a regulation, you’re not going to get very far with it,” says Atif Kureishy, Teradata’s global vice president for artificial intelligence and deep learning.

Fragmentation of Teams—and Therefore Siloed Data

In a panel discussion at the 2017 Money20/20 conference, Apple cofounder Steve Wozniak noted that the key to industry success will be investing in AI and building “centralized teams” focused on deploying it in ways that augment rather than replace humans.

Real-Time AI Deployment: Current Realities and Constraints

One reason that many rules-based systems are still in place is because they’re fast. Some types of transaction monitoring demand sub second decisions as to whether to let a potential transaction proceed. A collection of logical rules can execute very quickly. By contrast, some AI models can be relatively slow, involving potentially lengthy sequences of intertwined operations to produce a prediction and associated probability about a transaction’s legitimacy

Managing AI Models in Production

In addition to the challenges of getting AI models into production and delivering results at speeds fast enough to be useful, there’s the issue of monitoring and maintaining the machine learning models in production. The right tools do not yet exist. Numerous model governance issues are not yet adequately addressed by currently available software. If a model that once performed well starts behaving badly, possibly because the characteristics of new data no longer resemble the data the model was trained to handle, how do you quickly replace the model with one that will perform better? Are you monitoring the models in production, as well as a pool of candidate replacement models? Do you have back-up plans for redirecting data for scoring based on the observed performance of the production and challenger models? Are you able to redeploy models easily? All of these types of operational challenges hold across all models and are more significant than the actual development of any particular model.

Managing Alerts from AI-Based and AI-Enhanced Monitoring Systems

Although AI models dramatically reduce the occurrence of false positives, AI models still generate a large number of alerts requiring manual review. You need to consider how to most efficiently investigate those alerts. For example, if you receive an alert about a client engaging in suspicious behavior, you must thoroughly investigate that client, search for news about that individual, the client’s financial history, spousal and family relationships, and more. You’re gathering a lot of data, and then you need to make sense of it. This is where an emerging AI technology called robotic process automation (RPA) can help. When paired with AI models, RPA can accelerate the search for

and analysis of the large amounts of data relevant to alert investigation, relieving the burden from your human staff.

Other Operational Challenges

A number of other challenges with operationalizing machine learning models exist. Models can become “entangled” when one model begins to “consume” another model. Model entanglement occurs when you have undocumented dependencies between models. This can result in unexpected cascading effects that in turn produce performance issues that are difficult to recognize and resolve.

From Machine Learning to Deep Learning

As the team shifted its attention from more traditional machine learning to the development of modern AI models, it was able to use the analytics platform it had built during the machine learning phase to test and validate different kinds of deep learning, neural network architectures. Reimagining deep learning architectures originally designed for visual detection and object recognition as tools for making predictions with sequences of transactions, the team found substantial improvements in model performance. Com- puter vision models are some of the most advanced of AI models, having surpassed even human performance at identifying and label- ing objects, and doing it much more quickly and reliably: Danske Bank benefited from having an AI data science team able to trans- late the strengths of AI models designed for computer vision into a domain characterized not by images, but by sequences of transactions and transaction-related attributes.

The net result of applying the first iteration of AI models to the fraud detection use case, including computer vision and sequence models such as long short-term memory (LSTM), was a further 20% reduction in the false-positive rate—a significant improvement over traditional machine learning models.

A Platform for the Future

Through its partnership with Teradata Consulting, Danske Bank was able to build a fraud detection system that made autonomous, accurate decisions, integrated with existing business processes and systems, and met the bank’s requirements with regard to security, availability, and time latency.

For Danske Bank, building and deploying a custom analytic solution that met its specific needs and utilized its data sources delivered vastly more value than an off-the-shelf fraud detection product

because the custom models outperformed competing models and because they established the foundation of an agile platform for future analytics development and deployment.

With its enhanced capabilities, the solution is now ready to be used across other business areas of the bank to deliver additional value, and the bank is well poised to continue using its data in innovative ways to deliver value to its customers.

Conclusion

In closing, AI provides a new way forward to mitigate financial crime—a new way that goes well beyond the myopic concerns that have motivated anticrime efforts of the past.

Pleasing regulators is not enough.

Regulators can say you're doing a good job complying with regulations, but regulatory compliance is not a good measure of business success. Even with the late 2018 guidance from US regulators that companies should look to incorporate AI into their AML efforts, regulatory compliance isn't enough. Of course the advantage of a focus on compliance is that compliance is clear— indeed, AI and machine learning can help to automate business processes, including communications, to ensure that they systematically comply with regulation. It is appropriate that there are investments in operations to comply with regulations. How- ever, in spite of compliance with regulation, financial crime still costs businesses $4.2 trillion annually: it's clear that compliance with regulation is not synonymous with crime prevention. Instead of only responding to regulator guidance on what practices to implement, financial institutions need to discover, implement, and own the practices that go beyond compliance to prevent crime. They need to be proactive, to step up and define what good AML and fraud detection and other crime-fighting processes look like, to protect themselves against the crime that threatens to compromise the integrity of their services and brand.

AN ELECTIVE DEFENCE AGAINST FINANCIAL CRIME IS AN ELECTIVE DEFENCE OF YOUR BRAND

There's a misconception that the financial-crimes team does not contribute to the success of the corporate brand. Anticrime measures do not only protect against immediate financial losses. As soon as a financial institution's reputation for safety and security comes into question, shareholder and brand value take a significant hit. Every anticrime advantage you have defends you against lost revenue, lost customers, and lost reputation. AI-based approaches have demonstrated step-change improvements in the fight against financial crime. Defend your organization against crime like your brand depends on it, because it does.

Fighting Financial crime is the responsibility of the entire organization. In the past it was thought that IT or dedicated risk and compliance employees alone are responsible for the fight against financial crime. Given that financial crime represents an existential challenge to the operating model of the firm, everyone from the board of directors on down needs to treat it with the seriousness and common purpose that it deserves. The reality of fast evolving attacks by financial criminals demands

that institutions have methods shared across the organization to respond to attacks with three A's of accuracy, acceleration, and automation: AI is the best-performing approach to power a unified and ever-improving platform to deliver what the entire organization needs in the fight against financial crime.

Virtually all financial firms at this point are either deploying AI or planning to experiment with AI. The smartest executives realize that the swift and effective adoption of tailored AI will be one of the techniques that shape the future of financial services. AI will cut compliance risk, scrutiny from regulators, and, ultimately, cost. You won't get your name dragged through the mud. You won't get fined huge sums. And you won't have an auditor sitting at the next desk, watching your every move because you're under a consent decree.

The benefits of deploying AI to fight financial crime are broad and deep. The winners will be defined not by necessarily who builds the best models, but by who has the best data foundations and who has built analytics, engineering, and operational excellence into the very fabric of their companies to bring wave after wave of AI advances to the fight against financial crime.