INSIGHT

A.I. AS AN ALLY IN THE FIGHT AGAINST FINANCIAL CRIMES IN BANKING

A Brief Introduction

Artificial Intelligence ("AI") is the use of software applications - and sometimes specialized hardware - that utilize algorithms that make decisions similar to human cognition. Machine learning is a subset of AI which utilizes algorithms to "learn automatically" over time to enhance application outcomes with high degree of accuracy[1].

AI, notably Machine Learning, can help financial institutions reduce financial crime in the following ways:

- Reducing false positives to improve suspicious activity identification
- Increase the speed by which transaction layering can be uncovered
- Improve the accuracy of sanction screening and risk rating clients

In what follows, we will explore these methods, along with some recent examples of where AI may have helped combat against illegal activity in banking. We will touch on a few other opportunities to leverage AI in the struggle to maintain compliance in this regulatory environment.

AI In Action against Financial Crime: A Deeper Dive

- ## Using AI to reduce false positives and detect true suspicious activity

An effective AI system reduces financial and regulatory risks to financial institutions. Although rule based scenarios are efficient at managing high volumes of alerts, they are cumbersome and difficult to manage due to the volume, complexity and variety of data changes, or changes in the macro regulatory environment. Ongoing monitoring under rule-based scenarios can also be very costly for institutions to maintain. An alternative approach to consider is the utilization of Machine Learning powered algorithms, which adapt to data changes through self-learning and predictive contextual awareness and continual feedback, by building rules as they arise and tweaking the parameters as needed[2]. Financial institutions that leverage this approach for transaction monitoring and fraud detection become more capable of reducing the volume of false positives – enabling a sharper focus on truly suspicious activity.

- ## Using AI to increase the speed of uncovering layering and fraud

AI can also help reveal fraudulent customers who attempt to layer their funds by way of multiple transfers over multiple accounts, product types and geographies. The use of AI allows for greater transparency into the more complex and intricate web of transactions, uncovering links between entities and/or individuals which would not be easily identifiable by a human. To enable this capability, AI utilizes pattern-based segmentation of large amounts of transaction data, using these patterns to rapidly analyze and isolate factors which disguise of the parties behind complex transactions – thus revealing the true source and purpose of questionable activities[3]. The efficiency gained by linking and sifting through complex data allows financial crimes investigators to more accurately identify suspicious actors with speed, resulting in more accurate SAR (Suspicious Activity Report) filings, and thus improving the ability of law enforcement to act more quickly in the fight against financial crime. A capability such as this may have been beneficial for a major financial institution such as UBS, which was assessed a $14.5 million dollar fine in December 2018 due to poor monitoring of security accounts that were used for the purpose of moving funds rather than moving securities[4]. The use of Machine Learning may have aided the detection of inconsistent transaction activity within the brokerage accounts and allow the bank to proactively mitigate the risk of these accounts being used as conduits for illicit activities.

- ## Improving sanction screening and risk based decisions via AI

Fines amounting to billions of dollars have recently been imposed on major financial institutions, in part due to deficiencies in the current systems used by financial institutions to identify money laundering and other types of financial crimes. In April 2018, the Bank of China was fined $12.5 million by the Office of the Currency of Control ("OCC") and issued a Consent Order for deficiencies in the bank's overall compliance program and more specifically, due to deficiencies in its sanctions screening program. The sanctions screening program is a critical element of a bank's overall compliance program; therefore, shortcomings in this area can yield significant risks and exposures not limited to sanctions risks, but also reputational risk.

A key area that banks can explore for using AI to improve sanctions screening is the management of "good guy rules." Banks have traditionally used static rule based scenarios to create "good guy rules", which suppresses recurring names similar to names of sanctioned entities/individuals, but which have been identified to pose no sanctions related risks to the bank. When a name is suppressed, it will no longer be seen in the sanction filtering system. However, this process poses potential risk in the long term due the frequent update of the various sanctions lists and regulatory changes. Regular review of the "good guy list" should be conducted, but this a can be a very tedious, inefficient burden to financial institutions to allocate resources to facilitate this process.

The use of AI can help identify transactions that pose a potential sanctions violation by use of supervised Machine Learning, which captures patterns of data that passes through sanctions filters[5]. Using the predictive power of Machine Learning, the filtering systems can then further screen for suspects based on real time sanctions updates and those which have not yet been added to a sanctioned list but pose significant risk to the financial institution[6]. In instances of a true match identified during this process, banks can proactively self-disclose to U.S. OFAC and/or other relevant sanctions regulatory authorities, reducing the risk of

non-compliance and potential penalties. Financial institutions can then continually improve their ability to detect potential sanctions violations and money laundering patterns through self-calibrating models and unsupervised Machine Learning.

With the use of AI, financial institutions are also now able to make more accurate risk-based decisions before onboarding a client, thereby reducing financial, reputational, and regulatory risks. A real-time example of AI in action is the use of AI informed risk decisions, as part of the customer onboarding process. Traditionally, customer onboarding involves rules-based formulas to determine which questions a customer or prospect might need to answer, to satisfy risk scoring formulas. These formulas tend to be updated in current platforms manually, on a weekly or even monthly basis. Customer due diligence questions are then presented as part of phone outreach, email outreach or digitized web-based questionnaires. Leveraging AI, the questions could be determined "on-the-fly" based on a real-time risk score (vs. a stale manual model), assembled

automatically and then presented in either a call center or web-based questionnaire, to ensure Customer Due Diligence is completed with more current data, which minimizes compliance, financial and operational risk.

FIGURE 1. EXAMPLE APPLICATIONS OF AI IN ACTION TO COMBAT MONEY LAUNDERING
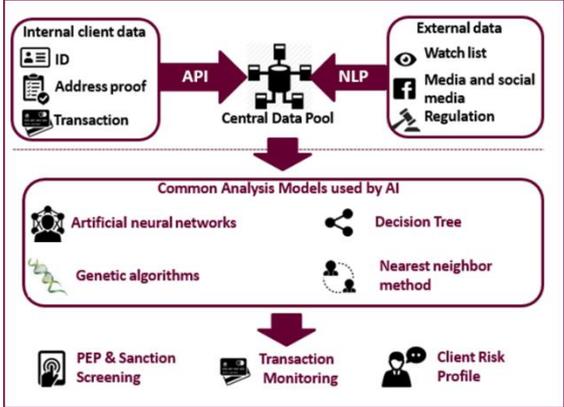
Source: Sia Partners

Other Opportunities to Leverage AI in the fight against Financial Crime include:

- Using AI for ongoing scanning and monitoring of social media and news sources in public and private Internet databases, to determine changes to the client's risk profile and risk exposures, and quickly react with controls due to negative news or other current data.

- Improving the identification of Politically Exposed Persons (PEPs)[7] and Ultimate Beneficial Owners (UBOs): Policies, procedures and controls must be implemented to mitigate against regulatory, sanctions and compliance risks posed by PEPs due to their inherent ability and influential power to misuse the financial systems and UBOs must be identified and verified at account opening and upon account review in-order to determine the true identity of all parties who maintains ownership of an account.

Recent News Examples Where AI May Have Helped – and is now Helping – Banks Avoid Crime

As evidenced with the number of regulatory actions imposed on financial institutions in recent years, regulators continue to focus on the compliance function of financial institutions. Some recent examples from the news include:

- In December 2017, Danske Bank was fined $2 million due to inadequate controls and the failure to detect "significant money laundering risks," associated with suspicious transactions that lead to money laundering activity[8]. More recently, in 2018, Danske Bank's Estonia branch was used as a hub for more than $8 Billion of transactions funneled into Europe through Azerbaijan, Russia and Moldova between 2007 and 2015[9]. This is a prime example of an opportunity where leveraging AI would serve to help detect suspicious transactions across branches and accounts located in multiple geographic locations.

- Deutsche Bank was fined for $630 Million a Russian money-laundering scheme which involved the bank's Moscow, New York and London branches. According to the New York State Department of Financial Services ("NYDFS"), Deutsche Bank failed to detect the movement of more than $10 billion in transaction into offshore accounts in a stock trading scheme involving its Russian clients' accounts.[10]

- HSBC is another example of a bank that recently used AI to update its financial crime policing capabilities. In 2012, HSBC was fined $1.9 billion for poor controls, which allowed Mexican drug cartels to launder money, and also violated U.S sanctions due to transactions involving Iran[11]. Over the last five years, HSBC has implemented steps to improve controls against money laundering, and has now incorporated the use of AI to increase efficiencies by automating its anti-money laundering function through the analysis of large volumes of data and transactions across their clients' wider network of relationships. This recent deployment of AI tools is now

further helping HSBC to reduce risk and cost in the fight against financial crime[12].

Recent Examples of How AI May also Help Banks Stay in Compliance

One of the additional benefits of introducing AI into operational use is the positive impact it can have on Compliance. A few examples include:

- A select group of banks have implemented the AI-driven "RegWatch Bot" that keeps track of financial regulations as they are being discussed, implemented or updated by national, local or industry group authorities. As a result, these financial institutions can stay up to date on new or potential regulation changes, and then redesign processes, policies procedures and internal trainings to help remain in compliance.

FIGURE 2. REGWATCH: AI AND MACHINE LEARNING BASED MONITORING OF REGULATORY CHANGES AND NEWS.
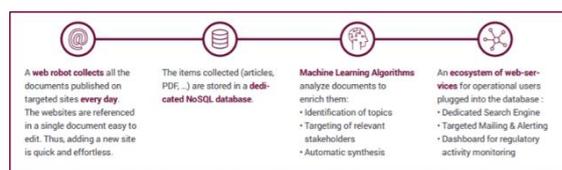
Source: Sia Partners

- The Commonwealth Bank of Australia recently utilized AI and natural learning processes to convert a high volume of paragraphs of regulations to compliance obligations with 95% accuracy conducted over two weeks – a task which would normally have taken well over six months[13].

Key Takeaways – and How Your Organization Can Get Started with Exploring AI

- AI can reduce financial crime by:
  - Reducing false positives to improve suspicious activity identification
  - Increasing the speed by which layering can be uncovered
  - Improving the accuracy of sanction screen and risk decisions

- AI can also aid with automating Customer Due Diligence questionnaire selection and related process digitization initiatives

- Other opportunities for leveraging AI in the battle against financial crime include:
    - Ongoing risk monitoring, using non-traditional data sets (such as social media)
    - Improving the identification and monitoring of PEPs (Politically Exposed Persons) and UBOs (Ultimate Beneficial Owners)
    - Helping financial institutions stay in compliance, via AI-powered monitoring of regulatory changes and related industry news topics

- Case studies from established global banks highlight that it is not too late to start your experiments to enlist AI and Machine Learning in your financial institution's own battles against fraud, money laundering and other criminal activity.

- Your organization can get started with:
    - A cybersecurity and risk assessment, to identify opportunities for improving your organization's anti-crime capabilities
    - The cybersecurity and risk assessment can be paired with an optimization and automation identification workshop, to reveal operational opportunities to introduce modern tools and techniques for combatting financial crime - including AI.

To learn more about Sia Partner's US offerings related to:

- Risk, Regulatory, KYC and AML – including Cyber Security –
Please visit
    - our US Website

For more information about Sia Partners offerings related to:

- Digitization Automation and AI
Please visit
    - our Data Science Lab
    - our list of Digital Assets
    - our Automation microsite

Sources

1. SAS (various authors). "Artificial Intelligence: What it is and Why it matters." Retrieved on Jan. 15, 2019, from SAS:Com at: https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html
2. Kumar, Anjura. "To truly transform KYC and AML operations adopt AI and ML…" Sept. 17, 2017. Retrieved from Finextra.com at: www.finextra.com/blogposting/14485/to-truly-transform-kyc-and-aml-operations-adopt-ai-and-ml
3. Ibid (same source as 2).
4. "FinCEN Assesses $14.5 Million Penalty against UBS Financial Services for Anti-Money Laundering Failures" via FinCen.Gov, Dec. 17, 2018, at: https://www.fincen.gov/news/news-releases/fincen-assesses-145-million-penalty-against-ubs-financial-services-anti-money
5. Long, Kimberly. "AI creates efficiencies in sanctions checking" June 16, 2016. Retrieved from via Euromoney at: https://www.euromoney.com/article/b12kq9zg21knmz/ai-creates-efficiencies-in-sanctions-checking
6. Kumar (source 2, 3), op. cit.
7. FATF Guidance 2013: "Polictically Exposed Persons, (Recommendations 12 and 22). Retrieved from FAT at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf
8. Reuters (various authors). "Danske Bank fined over money-laundering, says expands internal probe," Dec. 21, 2017. Retrieved from Reuters.com at: https://www.reuters.com/article/us-danske-bank-moneylaundering/danske-bank-fined-over-money-laundering-says-expands-internal-probe-idUSKBN1EF18P
9. Schwartzkopff, F. "Danske Fine May Be $670 Million as Analysts Look at New Evidence," July 11, 2018. Retrieved from Bloomberg.com at: https://www.bloomberg.com/news/articles/2018-07-11/danske-fine-may-be-670-million-as-analysts-look-at-new-evidence
10. Mullen, J. "Deutsche Bank fined for $10 billion Russian money-laundering scheme," July 31, 2017. Retrieved from CNN at: https://money.cnn.com/2017/01/31/investing/deutsche-bank-us-fine-russia-money-laundering/index.html?iid=EL

11. Silver-Greenberg, B. P. "HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering," Dec. 10, 2012. Retrieved from New York Times at: https://dealbook.nytimes.com/2012/12/10/hsbc-said-to-near-1-9-billion-settlement-over-money-laundering/

12. Irrera, A. "HSBC partners with AI startup to combat money laundering," June 2, 2017. Retrieved from Reuters at: https://www.reuters.com/article/hsbc-ai-idUSL1N1IZ1N3

13. Crozier, R. "CBA uses AI to make sense of regulations," Feb. 23, 2018. Retrieved from ITNews Australia at: https://www.itnews.com.au/news/cba-uses-ai-to-make-sense-of-regulations-485707

YOUR CONTACTS

DANIEL CONNOR

CEO USA
+ 1 (862) 596 - 0649
daniel.connor@sia-partners.com

FIONA LAYNE-GERMAIN

Senior Consultant
+ 1 (516) 296 - 0563
fiona.germain@sia-partners.com

CHRISTOPHER JOHANNESSEN

Director
+ 1 (484) 951 - 3792
christopher.johannessen@sia-partners.com

ABOUT SIA PARTNERS

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. With over 1,200 consultants in 15 countries, we will generate an annual turnover of USD 230 million for the current fiscal year. Our global footprint and our expertise in more than 30 sectors and services allow us to accompany our clients worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and we integrate the disruption of AI in our solutions.

Abu Dhabi
PO Box 54605
Al Gaith Tower #857
Abu Dhabi – UAE

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam -
Netherlands

Brussels
Av Henri Jasparlaan, 128
1060 Brussels - Belgium

Casablanca
46, Boulevard Adbellatif
Ben Kaddour, Racine –
Casablanca 20000 -
Morocco

Charlotte
101 S. Tryon Street, 27th
Floor, Charlotte, NC 28280,
USA

Doha
Al Fardan Office Tower #825
PO Box 31316
West Bay Doha - Qatar

Dubai
Shatha Tower office #2115
PO Box 502665
Dubai Media City
Dubai - UAE

Hong Kong
23/F, The Southland
Building, 48 Connaught
Road Central
Central - Hong Kong

Houston
800 Town and Country
Boulevard, Suite 300
77024 Houston, TX

London
36-38 Hatton Garden
EC1N 8EB London - United
Kingdom

Luxembourg
7 rue Robert Stumper
L-2557 Luxembourg

Lyon
3 rue du Président Carnot
69002 Lyon - France

Milan
Via Vincenzo Gioberti 8
20123 Milano - Italy

Montreal
304 - 19 Rue le Royer Ouest
Montreal, Quebec,
Canada, H2Y 1W4

New York
40 Rector Street, Suite 1111
New York, NY 10006 – USA

Paris
12 rue Magellan
75008 Paris - France

Riyadh
PO Box 91229
Office 8200 - 12, Izdihar city
Riyadh 11633 - KSA

Rome
Via Quattro Fontane 116
00184 Roma - Italy

Singapore
137 Street Market, 10-02
Grace Global Raffles
048943 Singapore

Tokyo
Level 20 Marunouchi
Trust Tower-Main
1-8-3 Marunouchi,
Chiyoda-ku
Tokyo 100-0005 Japan

For more information, visit: **www.sia-partners.com**

Follow us on **LinkedIn** and **Twitter @SiaPartners**

siapartners