External data sources: key inputs for compliance and investigations

Share | Tweet | Share

Whether digging through layers of a complex corporate structure to unearth the ultimate beneficial owners, conducting negative media searches or seeking to trace funds flow through a blockchain, the anti-money launderer (a new term?) will continually be referencing information outside their organization. ***Keith Nuthall*** *explores resources on offer – both free and paid.*

Enriched

RELATED

US securities regulator hits Raymond James and compliance officer hard for AML breaches

A virus, and it kills

Is it all worth it? – AML effectiveness

New wave – cryptocurrency risks

Down Mexico way

AML is all about the deft use of IT and the marshalling of data culled from financial records, but comprehensive KYC and client monitoring, as well as proactive ML investigations following up a suspicion, are aided by effective online tools that can uncover essential information.

Open and closed

Law enforcement, financial intelligence units (FIUs), private or in house investigators and anti-money laundering officers (AMLOs) in obliged entities may trawl open-source intelligence (OSINT) free or for a charge, or may access more restricted data, often for a subscription.

Mason Wilder, research manager, for the Association of Certified Fraud Examiners (ACFE), an international organisation based in the USA, said OSINT and automated data investigation tools used to probe predicate fraud crimes are also useful for ML inquiries. He stressed that these require the compilation of a financial profile of a subject, whether an individual or organisation, "and any AML investigators that are relying solely on internal sources of information are missing out on some potentially critical sources".

Bad news

A significant resource when utilising OSINT in AML reviews or investigations "is negative media screening", he told *MLB*, "[O]r, in other words, seeing if the individual[s] in question have been featured in any reporting that links them to illicit activities or known criminal actors or establishes them as a politically exposed person [PEP]." This can be achieved by search engine queries focusing on news results, although subscription databases, such as Dow Jones's Factiva [1], which compile researched material from different language sources, are very useful. Social media checks can help develop a subject's profile, documenting travel, lifestyle, assets, "and more that might suggest income beyond known sources". Tools that enable searches of various sanctions lists on one database are also very valuable for AML, not just to detect sanctions evasion, but "information about whatever sanctions regime an individual or a recipient of funds might be associated with can be an important piece in an AML subject's profile".

Free to pay

Commercial databases such as LexisNexis Accurint [2], TransUnion's TLOxp database [3], Thomson Reuters CLEAR [4] are also valuable for corroborating or verifying details an AML subject has provided, said Wilder. World-Check Risk Intelligence by Refinitiv [5] is a global database that can also aid KYC checks and due diligence, "but it can be cost-prohibitive for small organizations or individual practitioners", he noted. Free tools, such as Corporationwiki [6] and OpenCorporates [7], "are valuable for establishing links between organisations and individuals and for determining where companies an individual is associated with are registered so that you can get original copies of business filings", said Wilder.

Such techniques are of most use to law enforcement teams probing ML, said Tristram Hicks, director, Tristram Hicks Associates Ltd: "They are absolutely the ones that would be deployed by FIUs and law enforcement, particularly the latter," he told *MLB*. FIUs, he said, should only be using these techniques "to temporarily halt the transfer or recover the monies taken in the course of a crime in action", however. "It is important to distinguish financial intelligence from financial evidence, FIUs only do the former, competent authorities do both."

As for AML-obliged entity reporters and other private companies, "from a risk perspective, a client engaged in suspected dishonesty (fraud, corruption or other predicate crime) might well present a direct risk to the company, through defaulting or theft; whereas money laundering activity might be perceived as an indirect risk" worth investigating, perhaps with these techniques, although they can be expensive to deploy, he stressed.

OSINT at outset and beyond

Mr Hicks added that OSINT and other data checks do also have value for onboarding, but once the KYC checks are completed, he suggested, "the best source of information is what the customer does and the extent to which its activity with the company matches what the customer says it would do".

So, for KYC, this is where services such as "World-Check and social media have a role, to verify what the customer says about themselves", he said. At this stage, going further, such as undertaking dark web searches, would probably be "excessive for onboarding", said Mr Hicks. The same applies for ongoing corroborative checks of client activity, where "again, the customer is the best witness," he added. If something unusual is spotted, that is when companies should report suspicions formally via a SAR. From that point, "the risk is passed on", he said: "If law enforcement pursues the SAR, then they would generally go back to the reporter for more information. Normally, the reporter is a passive player, supplying SARs and cooperating with the competent authorities when asked to do so." And SAR suspicions can also be based on activities that do not require complex pattern analysis software to spot; for example, repeated transfers that are just below reporting thresholds, or multiple swift distribution of a large incoming payment, back-to-back purchasing of real estate: "Are these transactions so complicated to require machine learning to find? Perhaps, I guess it depends on the company's business," said Mr Hicks.

However, for those AMLOs who do want to go that further mile when undertaking CDD or checking to see if suspicions should merit filing a SAR or take other actions, Isabelle Birebent, Etienne Noel and Yong Li of Canada-based consultancy The AML Shop said external data sources have real value: "An AML officer should have access to the clients' behavioural patterns and intended use of the account/relationship, which should ideally include anticipated volumes, payment channels, frequency, sources of revenue/cash deposit, etc. Once these elements are known, it makes it easier for the AML officer to identify anomalies, outliers, and suspicious behaviour."

Here, Netherlands-based Social Links, for example, is one system [8] that could be useful. It touts itself as an investigative tool rather than a data collection service, saying it can integrate OSINT data harvesting with efficient inquiry management, highlighting relevant data, organising it efficiently and allowing investigators to collaborate, while checking and augmenting information. That can include money laundering evidence, especially via cryptocurrencies said a Social Links blog: "By applying OSINT technologies to explore blockchains intelligently, transactions can be linked to user addresses and assets can be traced to combat money laundering and mitigate financial risks," it said. [9]

Other tools and resources recommended by The AML Shop included using IP address look-up services, to verify the genuine geographical reach/location of an internet activity or actor. There are many such services, for instance that run by Neustar. [10]

Boolean logic

The AML Shop also recommends using 'Boolean' searches for searching open-source resources for negative news and other information on any search engine: Google, LinkedIn, or Facebook. "Boolean is a term used to define the process of combining keywords with words called 'operators'. These operators tell the search engine how to use the keywords in the search. Operator word examples are AND, NOT, and OR," said The AML Shop, enabling a researcher to limit or require specific results.

Here, searching news archives for stories that mention an individual or company "can help fill in gaps in your background information caused by incomplete online public records", and identify 'a pattern of behaviour, information that you would not pick up through other sources". The AML Shop's Birebent, Noel and Li, added: "Internet discussion groups (eg, Reddit) are a news source in their own right and postings may contain unsubstantiated rumours and gossip that may be worthy of further investigation."

Race around the block

External sources are also useful for virtual currency investigations, where an AML officer can use appropriate software for blockchain analytics and forensics, said The AML Shop, as well as for wallet screening, transaction screening and intelligence, "in order to detect patterns that may be indicative of an attempt at obfuscating the source or destination of an asset". UK-based Elliptic is one firm that specialises in this field. [11]

Birebent, Noel and Li added that another reason to use such tools would be to cluster multiple wallets, grouping a set of wallets to attribute them to a single entity. These tools can also help assess the level of exposure of a wallet or transaction to illegal or obfuscating services, said The AML Shop.

Web archaeology

Historic web data that is not unavailable might also be useful, said Birebent, Noel and Li: "assessing data that has been deleted from the Web" could provide valuable information, for example, using 'The Wayback Machine' [12], a digital archive of the World Wide Web founded by the Internet Archive.

As for the dark web, should investigators want to venture down this path, a set of useful tools are dark web search engines, which enable AMLOs to probe this unregulated corner of the internet, where – noted United Arab Emirates consultancy AML UAE, "money laundering is a common crime… as it allows the transfer of illicit funds to anonymous accounts." That often includes the transfer of virtual currencies, which, while often tough to trace, can be investigated. [13]

Dark web search engines include Finland-based Ahmia [14], and others, noted USA-based OSINT consultancy Brandefense. It said that Ahmia collects .onion URLs (those populating the dark web) from the Tor (The Onion Router) network and offers search results from any page lacking a robots.txt file blocking indexing. Another is The Hidden Wiki [15], which trawls descriptions of pages given in .onion links because domain names are changed often.

The AML Shop said: "Dark web investigations are useful. An AML officer can utilise a variety of sources whether open or subscription-based which may contain intelligence sourced from the dark web." It does however recommend that AML investigators cover their digital tracks when attempting to obtain dark web data, using, inter alia, anonymising services and proxies, such as VPNs (virtual private networks), and virtual machines (running in a window as a separate computing environment on a PC).

Find and join the dots

With sometimes unwieldy amounts of data available, one key role of IT tools is marshalling intelligence in a comprehensible way. France-based Linkurious [16], a data visualisation and analytics solutions service provider, says its systems can help investigators see the wood for the trees. That can be especially useful in tracking sanctions breaches, a complex field that has become denser following the flood of sanctions imposed on Russia following its invasion of Ukraine.

A Linkurious note said that AMLOs tracking such breaches could upload OSINT data from sources such as OpenSanctions [17] and the International Consortium of Investigative Journalists' (ICIJ) Offshore Leaks service [18]. "You can then define the topical structures as labels in a graph to see how entities relate to one another: politician, sanctioned entity, crime, terrorism, offshore, etc. Once your data is structured, you can start to search and explore," said Linkurious, which uses, as an example, Russian President Vladimir Putin. Its service can picture Putin's indirect links to offshore companies, culled from OSINT, to associates such as cousin Igor Putin or the Rotenberg brothers –wealthy close allies of Putin. "The connections you can see in the graph represent the beginning of an investigation. The technology is a great tool for building hypotheses that can be further investigated," said Linkurious.

Admissible evidence

For law enforcement, said Mr Hicks, assembling data gathered from such inquires could be useful later in formal proceedings or court: "An evidence gatherer would want to replicate the original discovery. Most reputable OSINT trainers can explain how to do this. The techniques are variations of screenshotting the discovery at the time and capturing metadata attached to a file," he said.

Ultimately, said Birebent, Noel and Li of The AML Shop, alternative sources allow anyone in AML – whether AMLOs or law enforcement – to double-check facts and find out more about a subject: "The use of data services that can cross-reference someone's address and their businesses can be extremely useful in drawing associations between individuals and ultimately discovering more about their activities. For example, the use of references provided by the ICIJ may give us better visibility into an individual's connections. If the data source is reliable/credible, then the facts/information gathered can potentially be useful for AML investigation and regulatory reporting…"

Notes

1. https://www.dowjones.com/professional/factiva/
2. https://www.accurint.com/
3. https://www.tlo.com/
4. https://legal.thomsonreuters.com/en/products/clear-investigation-software
5. https://www.refinitiv.com/en/products/world-check-kyc-screening
6. https://www.corporationwiki.com/
7. https://opencorporates.com/
8. https://sociallinks.io/
9. https://blog.sociallinks.io/what-is-osint/
10. https://www.home.neustar/resources/tools/ip-geolocation-lookup-tool
11. https://www.elliptic.co/
12. https://archive.org/web/
13. https://amluae.com/connection-between-the-dark-web-and-money-laundering/
14. https://ahmia.fi/
15. https://thehiddenwiki.org/
16. https://linkurious.com/blog/how-to-use-osint-for-aml/
17. https://www.opensanctions.org/
18. https://offshoreleaks.icij.org/

Mar 15 2023

Print this page | Send to a colleague | Email the Editor

Comments

TOPIC ALERTS

☑ Customer Due Diligence
☑ Monitoring
☑ Reporting
☑ Training
☑ Technology

Frequency: Daily
No. of articles: up to 10

Email Address: **timon.molloy@informa.com**

Manage topic alerts | Set up Alert

REPORTING

EU terror finance SARs set for US transfer

News

News

UK accountants win reporting exemption in privileged circumstances

TRAINING

The money launderer's bookshelf: part I

CUSTOMER DUE DILIGENCE

FATF targets Recommendations at tax and transparency

Latin lessons

News EU proposes zero threshold for sender data on money transfers

Contact Us | Help

Editor's Picks
PDF Archive
Advanced Search

Laundering
Customer Due Diligence
Law Enforcement
Monitoring
Record Keeping
Reporting
Tracing and Recovery
Training
Typologies
Terrorist Finance
Sanctions

Risk/Control
Alternative Remittance
Bribery and Corruption
Cash Seizure
Corporate Vehicles
Correspondent Banking
Internet
Payments
PEPs
Predicate Crimes
Proliferation Finance
Tax Evasion
Technology
Trade Finance
Industries

Regions
Africa
Asia-Pacific
Europe
Latin America and Caribbean
Middle East
North America
South Asia

Contact Us | Help | Terms and Conditions | Privacy Policy