Future Compliance: Envisioning a New, Smart Approach to Name Screening

By Beng Ti Tan and Nick Turner

We believe it is timely to re-examine the current industry baseline for the practice of compliance name screening from the bottom up. Emergent technologies such as artificial intelligence ("AI"), deep learning, and blockchain, among others, should be carefully assessed and applied to the screening function to make it significantly more effective, comprehensive, and accurate. The application of these technologies to digital transactions and payment systems also demands that the screening function become faster, handle higher volumes, and integrate with transaction systems in real time. The purpose of this short article is to begin to make a case for this re-examination by surveying some of the shortcomings of current approaches and sketching what a future architecture of smart screening might entail.

Today's Compliance: Name Screening Challenges

Since the early 2000s, name screening has become a staple function within compliance programs for most multinational corporations, financial institutions, and other organisations. Screening is used to identify individuals, entities, and countries sanctioned by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"), the European Union, or other authorities. It is also used to identify politically exposed persons ("PEPs") or persons named in negative media reports who may present corruption, money laundering, or other financial crimes or credit risks. Screening may also be used to identify other risky elements of transactions such as the involvement of controlled encryption technology, dual-use goods, or goods related to nuclear proliferation or military activities.

The cost of this function has steadily increased over time. According to one estimate, the five largest banks spend more than USD 10 billion annually on in-house screening capabilities, employing more than 50,000 employees.[1] Their role includes reviewing and responding to an endless stream of electronic screening alerts or "red flags" on customers, counterparties, and transactions, on a 24-hour basis. According to the 2017 Dow Jones and SWIFT "Global Anti-Money Laundering Survey", the increasing volume of false positive screening alerts was among the top challenges faced by respondents.

Content providers such as Dow Jones, Thomson Reuters, LexisNexis, and others have built a cottage industry on managing ever-growing lists and media databases to be ingested into screening software. They employ analysts, statisticians, researchers, and other skilled professionals to sift through, produce, and manage huge amounts of data. Regulators in many countries require screening as part of financial crimes compliance programs covering sanctions, anti-money laundering ("AML"), and anti-bribery and corruption ("AB&C"), among other areas.

Non-financial institutions have also invested heavily in screening tools. While the regulatory burdens are less onerous, non-financial companies, particularly manufacturers dealing in U.S.-origin goods, must ensure their products and services are not sold or transferred directly or indirectly to sanctioned territories or prohibited end users who appear on government-issued lists such as the Entity List administered by the U.S. Commerce Department's Bureau of Industry and Security ("BIS"). In Singapore and Hong Kong, financial institutions are increasingly asked to screen their trade finance transactions for dual-use and export control red flags.

Clearly, the complexity and expense of the screening function are significant, and likely to increase.

Expensive Errors

Apart from implementation costs, screening errors can lead to other costs, both in financial and reputational terms. Companies that are required to perform screening must do so diligently, or risk administrative or criminal censure.

Enforcement actions by OFAC and other government agencies provide examples of how failing to correctly identity and interdict prohibited transactions can lead to potentially expensive and embarrassing settlements:

- a European bank paid nearly USD 2.5 million after processing numerous USD transactions on behalf of companies owned by a Specially Designated National ("SDN") in violation of OFAC regulations. Information held by the bank's subsidiary in Africa was not made available in databases used by affiliates in Europe and the United States, preventing the identification of the prohibited payments. According to OFAC, the bank failed to update its screening filters in a timely fashion after learning of the deficiency, allowing additional prohibited payments to be processed;
- a US bank receiving a finding of violation for operating accounts on behalf of two SDNs. According to the settlement notice, the bank's screening software was not configured to compare dormant accounts against updates to the OFAC SDN List. Furthermore, the bank's staff failed to take

[1] *This figure was presented at the recent ACAMS annual conference in Singapore in April 2017.*

action to block the accounts even after becoming aware of negative media on the SDN accountholders;

- a US bank settled with OFAC for violations resulting from its failure to configure its screening software to detect geographic terms such as "Sudanese". In a similar case, a South American bank settled for violations that occurred when its software overlooked references to Iranian transactions due to a configuration error;
- In a landmark settlement in the UK early this year, an English manufacturer admitted to numerous counts of bribery conducted through (and in some cases to the benefit of) sales agents and intermediaries representing their aircraft engine sales business. Over the years, many of these agents were not subjected to background due diligence.

These examples highlight just a few of the typical challenges with current approaches to screening:

(a) First, systems that are improperly configured fail to identify obvious references to prohibited transactional elements, such as prohibited individuals or countries. This can occur, for example, when screening logic is too rigid to detect closely related terms (e.g. Sudan versus Sudanese).
(b) Second, human operators can fail to take appropriate action in response to screening hits by, for example, not blocking funds belonging to an obvious SDN or halting transactions to high-risk end users.
(c) Third, controls are implemented unevenly across disparate platforms and databases, even within the same organisation. This can occur when data in one system is not made available to another, or where decisions taken in one part of an organisation are not carried through to others. A bank that locates an SDN among its checking account customers should also review its credit card and commercial customers for related accounts, for example.

Beyond the risk to companies themselves, there are negative consequences for customers who must endure poorly designed compliance systems or wrong decisions. In 2007, the Lawyers' Committee for Civil Rights of the San Francisco Bay Area published a report entitled "The OFAC List: How a Treasury Department Terrorist Watchlist Ensnares Everyday Consumers" offering examples of consumers who were denied financial services because their names resembled those on the SDN List. The report highlighted the lack of safeguards to protect consumers from cases of mistaken identity involving SDNs. In 2017, the BBC reported that a US-based crowd funding website blocked funds donated to a UK food bank because of an issue with the site's OFAC procedures. These are just some of the cases that can be cited.

Underlying Constraints of Today's Approaches to Screening

We summarise the underlying constraints of today's approach to screening under four headings below:

(a) *Inefficiency:* Compliance screening today is a highly repetitive, manual activity. Escalating resources, both human and electronic, are being expended to crunch data and disambiguate potential matches. Take for example the sanctions screening function within a large bank. Customers are screened upon account opening and again periodically against updates to government-issued sanctions lists (among other lists). Each and every funds transfer is screened for references to sanctioned persons and territories by each of the originating, intermediary, and receiving banks. Screening alerts are raised to operations or compliance staff who must compare them against customer details and publicly available information to invalidate or confirm the potential match. The transaction or service is effectively paused (or should be) for the duration of these processes. All of this happens before any form of regulatory reporting, review, or investigation even takes place.

(b) *Diminishing returns:* Ironically, these resources are chasing a retreating horizon because, as the number of customers and transactions grow, especially electronic transactions, the proportion of potentially risky transactions is assumed to decrease. As anyone who has worked in a bank knows, transactions involving real SDNs are rarely found. Most potential matches are evidently false. Therefore, organisations are operating a screening system which they know will be overwhelmed by the volume of transactions sometime in the future—and that time is likely soon—yet with fewer tangible results to show for its expense and maintenance.

(c) *Data overload:* Another driver of cost is the size of data itself—electronic resources are severely taxed with ever more data to store, process, and analyse. Despite the growing amount of data available, traditional aggregative processing still applies rudimentary search principles that do not make deep or intelligent connections. Furthermore, decisions regarding potential screening matches are often not retained and recycled, meaning that similar searches and manual reviews are performed repeatedly.

(d) *Fragmentation:* The breadth and variety of data used in screening is relatively narrow and siloed compared

to the universe of data that is available. Internal data spread across an organisation's global footprint is not analysed holistically and is fragmented across different formats and file locations. Front-of-house and back-office data often is independent of one another. In the public sphere, web activity, social media activity, and online marketing/shopping are also generating large quantities of potentially useful data, but today's in-house screening systems are unable to ingest or process much of it as part of the name screening function.

To put a finer point on it, current approaches to screening are manually intensive, data inefficient, costly, and prone to errors, not to mention difficult on customers. These are all good reasons to explore new solutions.

Thinking Ahead

We believe a future screening system needs to address at least three critical constraints on current practices:

> *'We can't solve problems by using the same kind of thinking we used when we created them.'*
>
> *~Albert Einstein*

(a) The system needs to be able to accept and synthesize data of a wide variety of formats and types from various sources. Governments happen to issue screening lists in the form of text. And banks happen to screen text in customer and transactional data. But this misrepresents the "real world" of data available to a smart screening system. Microsoft Office documents, handwritten forms, audio recordings, social media, instant messaging, and all forms of internet publications, among others, are potential sources of information. Current systems are limited to a single dimension of data. Not only is this the one dimension that the targets are trying not to operate in, but it excludes opportunities to find identifiers for the purpose of disambiguation. This is especially true as digital transactions grow in popularity, crisscrossing regulatory jurisdictions and platforms where asymmetrical data is the norm.

(b) Current screening systems produce potential matches based on direct logical sequencing of data, with some fuzzy logic. Potential hits represent direct or near direct associations in data points. This means that software can easily overlook transactions that would require closer human scrutiny. Moreover, screening is limited to data which is proximate or homogenous in time and place. This paradigm will soon be—if it is not already—outmoded, as expectations for integrating data globally and instantaneously grow. Future-proof systems need to be able to apply Big Data solutions to improve access, processing, and archiving of large amounts of relevant information across data sources. Future systems should be able to draw information from across an organization's data stores and smartly extract information from contracts, logistics records, and other sources.

(c) Future screening systems also need to be designed with the rise of blockchain in mind. The move toward blockchain represents a broader trend towards transparent, validated transactions with parties sharing previously asymmetrical information in such a manner as to create auto-resolving and auto-verifying transactions. In contrast, screening systems today are disconnected from, or bolted onto, transaction systems. The two require human coordination to align. We believe compliance screening increasingly will need to integrate with blockchain systems in at least two ways. First, gatekeepers will need to authorize blockchain participants to access a specified blockchain platform. This is comparable to know-your-customer procedures today. Queries of the counterparty ledger as a source for screening data will also reduce the need to repeat screening processes. Second, screening systems must seamlessly identify and halt transactions belonging to participants who have access to the blockchain. This is comparable to transaction screening today. This optimally must be done rapidly and with minimal human interaction.

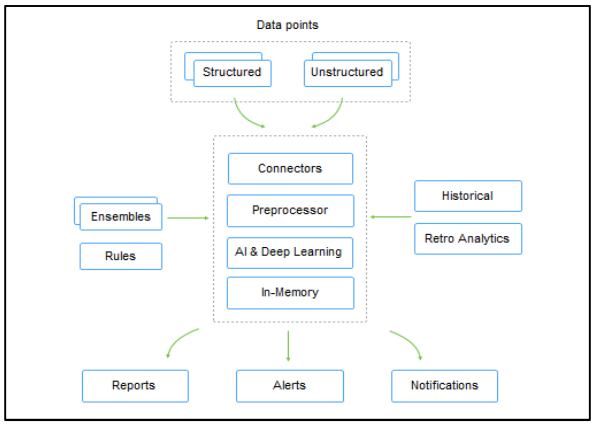
New Building Blocks

A survey of technology available and in commercial use today provides us with the building blocks for a screening system of the future:

- *Multi-format, real-time data collection and input*. Using an array of hardware and software input options, data of a much wider variety than today can

be collected and prepared for analysis intelligently and with speed. Optical Character Recognition ("OCR") has progressed to mimic the methods humans use to read documents and text, allowing critical information contained therein to be extracted and stored. Publicly available data on the internet is available for automated harvesting to increase accuracy and provide context for name matching.

- *Big Data Storage*. Today's Big Data solutions can provide smarter storage of data for quicker retrieval and identification. This is already being rolled out within many organisations and by storage providers such as Microsoft Azure and Amazon Web Services. Screening platforms need to be able to integrate with these repositories and also utilize them in storing screening results for future re-use.
- *Screening AI*. A variety of learning AI modules (some even in the open source realm) are available to be applied to the logic of screening. The technology can perform at least three transformative actions: (i) shift screening from a noun-and-phrase approach to a relational-and-context approach, producing much better and more meaningful results. (ii) AI can learn the sequence and logic of searches conducted by human operators and replicate them. Over time, it can generate searches independently based on historical searches. (iii) AI is able provide timely alert notification and make transactional interventions based on a relational and contextual matching of red flag indicia.
- *Neural Mapping Interfaces.* As opposed to current tabulated data outputs, future systems will present an organic mapping of red flags and regulatory requirements to provide a richer result, capturing more useful information gleaned from bigger data and smarter searching, with less effort and processing time than today's systems.



- *Automated Transaction Integration.* Screening systems need to be designed to integrate with transactional systems, like blockchain. Technologically, it is possible to run a screening blockchain internal to an organization and bridge its output to a transaction blockchain. Nowadays, designing any screening system that is standalone is building in obsolescence.

Conclusion: Tomorrow's Compliance

Through updated system design and automation, it is possible to minimize human input and the attendant inaccuracy. Self-learning tools can improve the disambiguation process and reduce the need for manual reviews while digitizing institutional knowledge and practice. The integration of decision outputs with payment platforms can improve coordination of compliance across business lines. The technological tools for better screening are rapidly coming into being. Practitioners, especially in the legal and compliance fields, are just now beginning to coalesce around a set of opportunities and a shared vocabulary for these new approaches. The business case for doing so is evident. Smart screening is coming into focus. The question for General Counsel, Compliance Heads, and Senior Risk Executives: is your organisation's next screening system designed to be smart and futureproof?

* * *

The views presented are the authors' and do not constitute legal advice, nor do they represent the views of the authors' respective employers.

Beng Ti Tan is Head of Compliance, Asia at Fujitsu, based in Singapore. Nicholas Turner is a lawyer with Clifford Chance in Hong Kong, where he is a member of the firm's economic sanctions and financial crimes practice.