# Banks turn to software to ease stress as regulations tighten around the globe

Emma Dunkley

©Yuri Arcurs/PeopleImages
Voice alert: software can monitor conversations in trading rooms

Revelations about offshore accounts around the world, designed to shelter billions of dollars from tax, have thrust financial regulation into the spotlight.

At the heart of the Panama Papers were banks and financial services firms that had hatched thousands of shell companies in murky territories for clients, as revealed in files leaked from law firm Mossack Fonseca.

The debacle exposed how legal corporate structures were abused to enable money laundering and tax evasion in some instances. It highlighted a big challenge for banks: the need to tighten checks, controls and more effectively police customer data.

Experts believe banks will increasingly turn to external technology providers to help them comply with a mounting regulatory burden.

Financial services providers are under pressure to stop abuse and comply with a stream of regulations that vary across jurisdictions. These range from anti-money laundering rules to country-specific regulation such as ringfencing in the UK, which requires banking groups to hive off their retail arms from riskier divisions by 2019.

Most recent reforms have come in response to the 2008 financial crisis. In the UK, the bank levy was created in 2011 to make banks contribute to economic recovery. The Dodd-Frank act in the US aimed to lower risk in the financial system with measures including a requirement for banks to have contingency plans for a quick and orderly closure.

"There are huge regulatory costs and overheads, which are something of an issue for banks," says Cliff Moyce, global head of finance practice at technology consultancy DataArt. "Banks are using screening software, plugging in extra IT tools to core systems to pick up any activity that might not be compliant . . . you don't want to screen everything but you don't want to miss anything."

In the UK, more than 80 per cent of banks' technology budgets for the past five years have been spent on addressing regulatory requirements, mitigating litigation and streamlining, according to estimates from consultants KPMG.
In 2013, the Basel Committee released its principles for risk-data aggregation and reporting after it found banks had been unable to efficiently quantify their exposure to the collapsed Lehman Brothers. In the US, the Office of the Comptroller of the Currency issued "heightened expectations" to enhance the risk management practices of large national banks — including a focus on data and reporting.

Banks don't want to have 10 different sets of regulation technology

- Bruce Laing

The Panama Papers leaks highlighted the need for banks to have strong "know your customer" checks in place and the ability to find information quickly for regulators. The UK's Financial Conduct Authority gave banks about a week for urgent reviews looking into whether they were linked to Mossack Fonseca.
Plugging in third-party technology requires banks and financial services companies to have sufficient customer data, without which the software cannot screen for anomalies or areas that do not comply with regulations. Any instances of insufficient data would require reinputting client information, wasting time and resources, says Joe Cassidy, partner at KPMG. For example, documents such as passports must be scanned, kept in a database and be easily retrievable. But third-party software adds to costs for banks already suffering from lower profits and fines for behaviour such as mis-selling mortgage-backed securities and rate rigging. And their systems can be old and complex.
Bruce Laing, partner at consultancy Deloitte, says: "There are lots of regulations in many different jurisdictions, but a lot of the technology only focuses on one problem. Banks don't want to have 10 different sets of regulation technology." He says some technology vendors are writing artificial intelligence programs that aim to create a single compliance software.
Increasingly sophisticated programmes are being developed. One type used by various banks, especially those with trading divisions, is voice surveillance. Some consultancies have developed a technology that can capture voices across the trading floor, take recordings and match conversations against lexicons to highlight anomalous words or patterns. This can send an alert to prompt human intervention. This process means that someone is not burdened with listening to all conversations.
Scott Weber, managing director of cyber-risk specialist Stroz Friedberg, says: "Communications can show increased levels of stress and disgruntlement and could highlight the potential for someone to do something risky."
As the Panama Papers affair has shown, businesses need strong customer checks and clear processes for using data. Technological developments offer banks and finance companies more tools to comply with an increasing number of rules.

Original article — http://www.ft.com/cms/s/2/7bfd4794-0095-11e6-99cb-83242733f755.html - axzz4AL4VaCCD