

HORIZON

from
SKADI

Damian Taylor 

Dave Bridges 

April 2023 Edition

- **The devil is in the detail**, knock-on effects to consider operationally as clients seek new deposit facilities after various US bank failures.
- **Oi...oi...AI** ... thoughts on generative AI and Internal Audit functions.
- **Times, they are a changin'...** both USD LIBOR and Dated Brent benchmarks are set to change in the coming months.

The month in review

At the start of April, the Prudential Regulation Authority (PRA) made an [announcement](#) regarding regulatory inadequacies at Wyelands Bank. These lapses include the bank's inability to establish document retention and record-keeping concerning instant messaging platforms, with a specific reference to WhatsApp. This is the first time that we have seen the UK regulators issue fines regarding WhatsApp messaging, although there have been several large fines issued from the US regulators over the past 2 years which we have highlighted previously in Horizon. We expect this area to remain in focus with UK regulators.

Following JPMorgan's takeover of troubled First Republic Bank, coupled with the failure of Silicon Valley Bank, it is worth considering the operational knock-on effects for banks on the receiving end of new clients looking for a new home for their deposits.

A similar situation occurred some years ago, as Dave Bridges, SKADI's Operations SME explains:

"When certain countries were downgraded in the Eurozone crisis, the Spanish bank I was working at needed to on-board clients into London and set-up a deposit-taking facility from a blank canvas, as quickly as possible!

When we consider the fact that funds can't be migrated until client onboarding set-up is completed, Customer Due Diligence (CDD) and support functions will be placed under considerable pressure. A single client may take deposits over several sub-funds, which all need to be scrutinized and onboarded. In my case we needed to take on over 1,000 accounts, depositing several billion pounds. The numbers in recent events are surely much larger!

For each account, questions still need to be considered. Does deposit-taking match the profile of the client? Are the funds visible on their balance sheet? Is the client eligible for the FSCS (in the UK) or FDIC (in the US) cover? If so, has this been flagged correctly in static data fields, and have details of the scheme been disclosed to the client?

Operational impact is also important to consider. In my example, operations functions had to support new requirements which included: automated SWIFT messages (MT54x), daily file uploads to confirm balances, daily email reports showing account balances, and periodic confirmation of compliance with client money rules set out by the FCA.

Finally, the nature of the new transactions created should be considered carefully: do the new clients format their SWIFT messages correctly to prevent manual intervention? Do their settlement instructions contain certain keywords which cause payments to hit SWIFT screening software requiring review? Are redemption requests made close to currency cut off deadlines?

Whilst deposit taking may easily be perceived as the bedrock of banking, as highlighted, the devil is in the detail.”

Forward-Looking

Oi... oi... AI

Type “AI and Internal Audit” into your search engine of choice, and you will be hit with a barrage of articles about how AI is going to be a “gamechanger” and will “turbo-charge” audits. This may, or may not, turn out to be the case, but the rise of the AI productivity tools such as ChatGPT is going to bring with it a whole host of issues around privacy and confidentiality. As an example, much of the work that we do in and around Internal Audits and Investigations is centred around the report writing that occurs at the end of the process, and the “selling” of audit points and findings to senior management. Who wouldn’t be tempted to ask ChatGPT to “write the following paragraph in a more clear and concise manner”, but where could this internal, sensitive information end up?

“The issue of confidentiality of internal information is a valid concern when it comes to the use of generative AI for internal audit functions. Generative AI models typically require access to large amounts of data in order to learn and generate new content, which can include sensitive and confidential information. This raises the question of how to ensure the security and confidentiality of this data, and how to prevent unauthorized access or use of this information. To address this issue, organizations must implement robust data security measures to protect confidential information. In addition to these technical measures, organizations must also ensure that their internal audit teams are properly trained on data security best practices and are aware of the risks associated with the use of generative AI.” [a ChatGPT query on confidentiality of internal information!]

Much like the normalisation of the usage of instant messaging forms of communication, such as WhatsApp, have proved a headache for the banks to police, we can foresee similar problems with access to generative AI, which will become more and more ubiquitous. Blocking access to AI websites on corporate networks and over WiFi can still be circumvented on personal devices via mobile networks, or via VPNs. It will be key for new policies to be in place (if they are not already!) to deal with the usage of AI in the workplace and, just as the recent DOJ [statement](#) articulates regarding instant messaging, having a policy is NOT in itself enough. From Section II, page 9: “...Prosecutors are

instructed to probe specifically whether a compliance program is a “paper program” or one implemented, resourced, reviewed, and revised, as appropriate, in an effective manner.”

Two up-coming areas of focus in markets.

Internal control functions need to be vigilant over upcoming major changes taking effect over the coming months:

- In early April the FCA [announced](#) their decision on USD LIBOR. ICE Benchmark Administration Limited (IBA), will continue to publish a synthetic methodology “synthetic US dollar LIBOR” for 1-, 3- and 6-month rates after 30 June 2023 with an expected cessation on 20 September 2024. The publication of synthetic US dollar LIBOR is intended to be used for legacy contracts only.
- From June, dated Brent the underlying contract for Brent futures, will also include US WTI Midlands crude in the S&P Global Platts Brent oil benchmark. This additional grade of crude will be the first from outside the North Sea to be included from 11 US Gulf Coast terminals.



The SKADI Podcast - Rogue Trader - Barings

Coming soon...!

The shocking story behind the collapse of Barings Bank in our new podcast episode of, "The Rogue Trader Chronicles."

Follow the web of deception and corruption that led to one of the most significant financial scandals in modern history. Join Skadi's team of experts as we unravel the intricate details and discuss the lessons learned from this catastrophic failure.



SKADI



enquiries@skadilimited.com

www.skadilimited.com