Dave Bridges Nicolas Corry Damian Taylor

June 2023 Edition

In this month's HORIZON:

- **Wholesale banks and cyber risk for data and models**
- **Culture risks in financial institutions**
- **Russian ADRs – reconciliation of ADR versus local**

Increased threat of hacking to financial institutions

The recent headlines concerning the MOVEit hack, as more and more institutions admit that they have been breached, gives us pause for concern on another risk of hacking, and one that financial institutions, and the control functions within them, should be alert to.

The MOVEit attack has been about the harvesting of personal data – stealing names, addresses, social security details etc… to then enable criminals to clone, phish, exploit individuals. However, there are other vulnerabilities that reside in wholesale financial institutions that hackers might also look to exploit.

At the core of financial institutions sits terabytes of data – pricing data, static data, payments data, proprietary data, transactional data etc… and on top of this data sit a multitude of proprietary models that allow the bank to price up complex derivatives, run risk metrics and the like. Banks obviously have very strong controls in place to ensure that this data is protected, but could they be vulnerable if they were somehow hacked?

As we enter a period of increased geopolitical tensions, with the Russia-Ukraine war entering a new phase, and a general sense of unease between Washington and Beijing, what better way for hackers to look to destabilise the status quo by going after financial institutions – the cogs that sit at the heart of the modern capitalist system?

Further, in the past couple of decades, the nearshoring opportunity of using cost-effective Russian-based programmers with very strong programming skills means that there is intimate knowledge of many of the models used by financial institutions in the wholesale markets, and their associated potential vulnerabilities.

With US Presidential elections next year plus a raft of elections in some of the major Western nations, the chance of destabilising actions by hacking groups will continue to persist.

Where does this sit within the framework of control functions and internal audit within the banks? We argue these concerns should be front and centre. An attack on wholesale banks – at either datasets and / or models should be a huge concern.

If we were in internal audit, we would be asking what considerations business lines are putting towards a cyber-attack, and what contingencies are in place if an attack were to occur either effecting internal systems OR if an attack were to occur to a large competitor bank?

Pie in the sky thinking? We think not. Consider the issues caused by the hack into ION (not a bank, just a software vendor!) that caused a mass scramble by back-offices to resort to manual processing of trades (see Horizon Feb-23) and the several-day delay of the calculation of the COT report. Also, think of the knock-on effect of the gilt sell-off on LDI positions – margin calls compounding problems. Imagine the damage that could be done with a sharp sell-off in the US Treasuries market – the pristine collateral that sits at the bedrock of many financial deals. Finally, let's not forget that Knight Capital was put out of business when a trading algorithm that was supposed to trade a portfolio of stocks over several days ended up trading billions of stock over an hour. Although the last was obviously NOT a hack, it is important to understand the risks to a firm and also the integrity of the market from an errant model.

Culture risks in financial institutions / NDAs

It was reported in May that Goldman Sachs would settle a decade old class action with 2,800 women. In recent years a number of banks have found themselves dealing with the fall-out from arrangements with convicted sexual offender Jeffrey Epstein. Last month Crispin Odey was forced to step down from his leadership of Odey Asset Management. Allegations against Odey now stretch back as far as 1985, as more women come forward to make allegations against him. Away from Finance, the BBC is examining their own handling of allegations made against a presenter. In May 2022 the Guardian newspaper listed 14 sexual misconduct allegations against MPs. Since then, further allegations have come to light.

The Goldman Sachs out of court settlement, purported to be US$215m, along with the settlements agreed between JP Morgan and Deutsche Bank and lawyers for Epstein's accusers, reportedly US$290m and US$75m respectively, gives an idea of the size of potential legal risk residing within Financial Institutions.
This potential legal risk is signposted by historic agreements signed between parties. We are, of course, referring to Non-Disclosure Agreements (NDAs). Attitudes to the use, or rather misuse, of NDAs are changing. The Legal Services Board has signalled their intention to beef up their response to misuse of NDAs, citing a need for a "strengthened and harmonised regulatory approach". The move by the Legal Services Board reflects a willingness for victims to test NDA enforceability. The #metoo movement has been a principal driver for change.

A freedom of information request made to the Financial Conduct Authority (FCA) in 2021 revealed that the FCA had at that time prohibited 4 individuals as a result of finding them not to be fit and proper. The Crispin Odey scandal has seen the FCA questioned by the Treasury Select Committee with regards to what they knew when. The Treasury Select Committee also asked about
Non-Financial Misconduct in a wider context, asking:

"*What systems are in place at the FCA to deal with accusations of non-financial misconduct by individuals in financial services? To what extent is this a priority for the FCA? Has the FCA undertaken any wider work on non-financial misconduct in financial services?*"

In the past SKADI has pointed to the example of eradicating sexual harassment to illustrate the challenge faced to change culture within organisations. It seems apparent to us that there will be a concerted ramp up in scrutiny and a desire to see evidence of results in the very near future. For Financial Firms in the UK this drive will likely be spear-headed by the FCA.

One immediate way Control Staff can help their institutions get a measure of potential risk they could be exposed to, is to conduct a historic review of NDAs, and whether these relate to Non-Financial Misconduct. Additionally, reviewing compromise agreements signed with employees when they have left the firm to understand whether these have "silencing clauses" in relation to Non-Financial Misconduct. It seems likely that Insurers will be of the view that they face increased potential liability, and being able to evidence to the firm's Insurer will mean that some cap can be kept on inevitable increases in premiums.

Russian ADR's – reconciliation problems of ADRs versus local holdings

Russian ADR (American Depositary Receipt) owners are facing significant challenges as a depository has informed owners that they cannot guarantee access to the underlying Russian shares that rightfully belong to them. The issue arises from discrepancies in the equity positions held in Russia at a different depositary bank, which correspond with the ADRs. The situation stems from Moscow authorities who allowed investors to "convert" their ADRs into local shares, thereby delivering local underlying shares directly, bypassing the involvement of the depository. This leaves the depository with the task of reconciling the shares settled to the owners against the outstanding depository receipts to resolve the issue.

Russia's National Settlement Depository said the conversion of shares were performed in accordance with Russian legislation and that they were not responsible for implementing this mechanism. The conversion process was called "complete chaos" by lawyers, with one lawyer citing the current reconciliation breaks could reflect that a holder owns both the ADR's and the underlying shares.

As Dave Bridges SKADI's operations SME explains: *"In normal circumstances, ADR's can be delivered from Euroclear or DTC and the underlying shares received the following day. Upon receipt of the Depository Receipts and any legal documentation from the holder, the depository can mark down the issuance of ADR's and instruct their local correspondent bank to deliver the underlying equities to the holder's local custodian.*

This unusual situation of underlying equities being delivered without the depository having line of sight may reach to the other 3 depositories who collectively sponsor 69 Russian ADR listings. These challenges highlight the need for inventory positions with local custodians and with Euroclear and DTC to be watertight and for corporate action teams to remain alert to any notifications of further developments."

Index for previous Horizon editions
Scan the QR codes below to view each publication.

February 2023
We analyse the marking of assets with embedded interest rate risk

April 2023
The implications AI creates for internal audit functions

May 2023
We reveal the operational impact of currency restrictions

November 2022
Marking into year end, areas of focus for control functions

December 2022
Explained in this edition: How do back-to-back bookings and settlements work?

January 2023
Valuation methodology: We explain where risks can hide and highlight areas to review

The SKADI Podcast – The Greek Debt Crisis

Coming soon...!

We are all familiar with the Greek debt crisis that started in 2009. The fallout was far-reaching, impacting large international organisations and causing the European Union to step in.

How exactly did everything happen? What went so wrong and why was Greece known as one of the worst economic crises in history?
Join SKADI's team of experts as we take a deep dive into the intricate details and analyse the lessons learned.

SKADI
enquiries@skadilimited.com
www.skadilimited.com