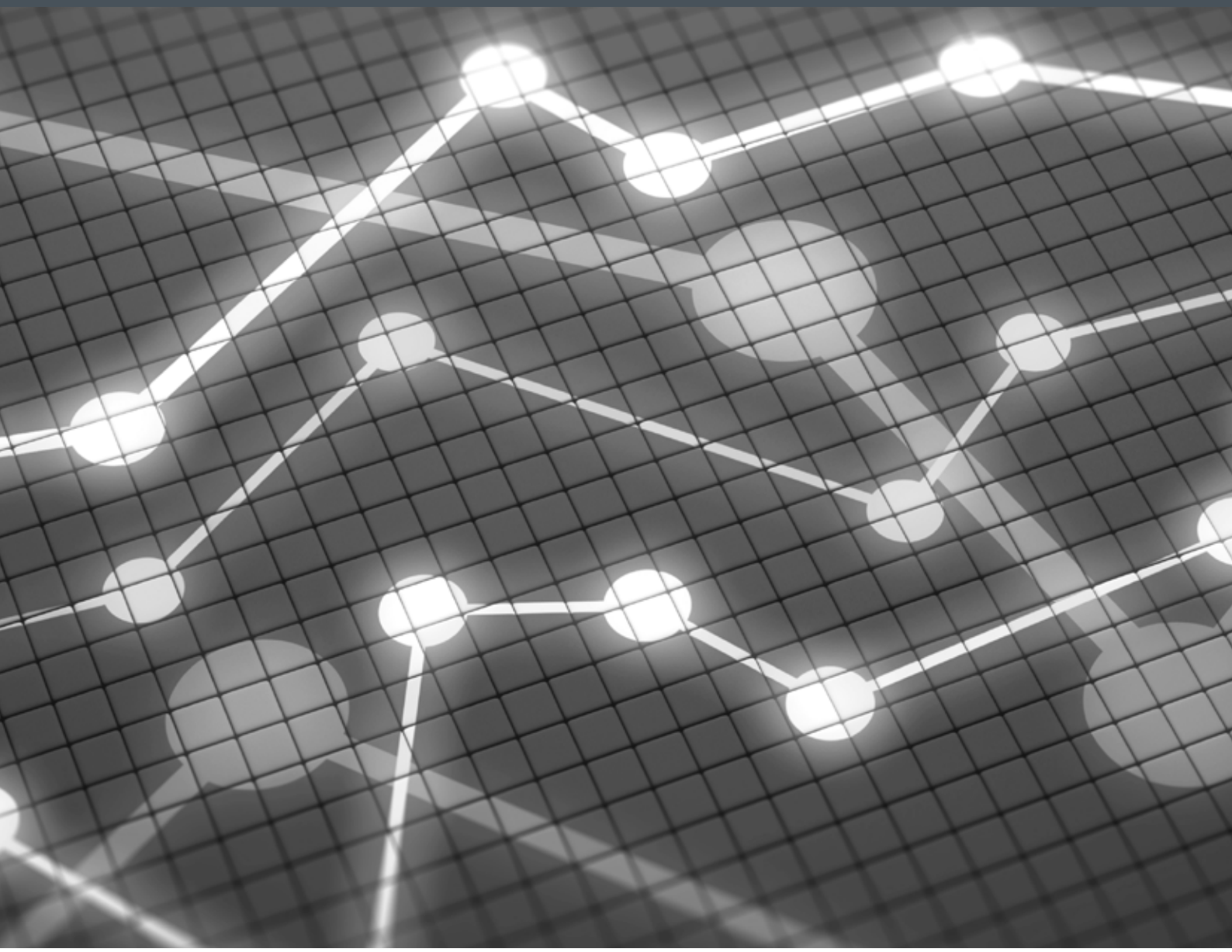


FINANCIAL LINES AND COVID-19 - UPDATE

In our previous article[1] we wrote about areas where we saw potential risks for (re)insurers of banks in GCC countries. Given the fast moving nature of COVID-19 and the response of the various authorities, we now consider further developments.

Our initial thoughts were concerned with areas where we thought losses/claims would arise (e.g. bank operational risk policies, loss of data). This briefing addresses risk mitigation.

1 https://www.hfw.com/Financial-Lines-and-COVID-19-Mar-20

> **“Simply put, the failure to have adequate processes in place can, at best, delay payments under a crime policy.”**

Crime

As we noted, working from home can result in dilution of internal controls, exacerbated by fewer people on the bank premises to process transactions. So, how does this work with banker’s blanket bond (BBB, or crime) policies from a coverage point of view? Some bank crime policies contain express requirements as to dual control (either in the proposal form or in the policy itself and generally expressed as a warranty) and the dual control requirements are particularly set in GCC countries (where policy wordings continue to be written on old, London market, wordings, some harking back 40 years).

Thus, where a loss occurs and is, on its face, due to a lack of dual control, the cause of the loss needs to be carefully examined given that in most GCC countries there has to be a nexus between the breach of the warranty (i.e. there is dual control maintained over transactions) and the loss/claim which has occurred. Notwithstanding this, there is no substitute for internal controls and back office due diligence (for example where proprietary trading is taking place). Simply put, the failure to have adequate processes in place can, at best, delay payments under a crime policy.

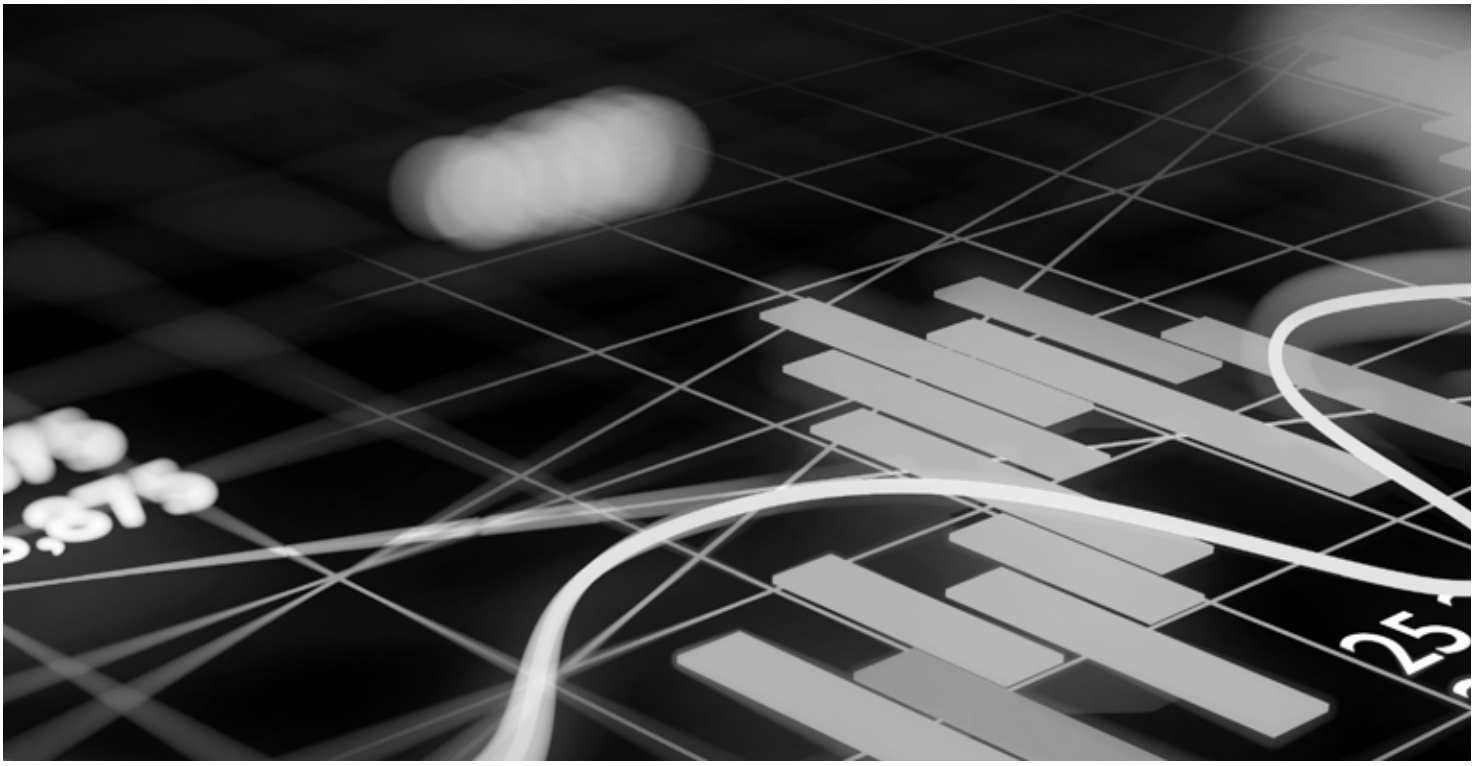
Another area where we see many risks occurring is in terms of funds transfer instructions received from customers. Whilst, more often than not, indemnities are given by customers who wish to utilise email or telephonic instructions (such as to absolve the bank of any blame if such instructions are intercepted by fraudsters); nevertheless, overlying this with a “confirm” or call back requirement is likely to reduce the risks of such losses occurring.

However, notwithstanding the absolution requirements which banks protect themselves when offering a confirmatory facility, the practice in this area tends to get confused – call backs are introduced and, often, the customer’s indemnity is made conditional (expressly or impliedly) on the call back. Thus, a bank which agrees to carry out a telephone authentication process may leave it open to claims if the process is not carried out (albeit this can be dealt with in a contractual way). Whilst the bank can absolve itself from liability, it might save itself considerable time and (irrecoverable) defence costs were it to, for example, randomly select certain transactions or apply some form of risk assessment to transactions (and make it clear that it assumed no liability).

Trade credit/finance

With regard to trade credit/finance policies, banks should obviously be liaising with their customers to ensure that compliance with terms and conditions of the underlying policies are met. In our experience, it quite often comes as a surprise to banks who are designated loss payees under trade credit policies that insurers raise defences of non-compliance regarding the terms and conditions as against the policy holders (i.e. the customers). Banks are in no better position regarding their security under the policy than the customer, unless they have financiers endorsements attached to the policy. These endorsements provide considerable security to the bank, although many banks refuse to become co-insureds under the policy because they believe it is too much effort (it’s not!).

Whilst we note that banks’ abilities to monitor situations in the current circumstances becomes more difficult (given the lack of staff), so does it for their customers and the appropriate limits and notices may well not be given in a timely fashion under these policies – thus, exposing loss payees to non-payment or delay risk.



Cyber security and data privacy

As branches close and internet banking and the usage of mobile phone apps increases, the risk to banks of the theft of money and/or data, particularly personal data, is heightened. Cyber criminals are increasingly targeting all manner of businesses whose staff are working from home, and may already be feeling vulnerable and anxious as the Covid-19 peril accelerates, and banks are no exception. Rather, banks are particularly vulnerable given their very nature of their financial essence.

In addition to the risk of financial and data loss, home-based data controllers and data processors are no doubt experiencing a demanding time as they strive to stay on top of the requirement to collect, process and share additional amounts of data borne out of Covid-19 related issues.

There are however a number of basic steps which banks can take to mitigate such risks and protect against the loss of money and data:

- Ideally, create a home environment for key employees that resembles the office environment (with equipment) as much as is possible.
- Ensure that IT and security employees are readily and easily contactable and have the appropriate bandwidth and capability to cope remotely with an increased workload.
- Heighten data access controls and restrict access where possible.
- Provide adequate training to staff and remind them of the need to be vigilant in the face of increased phishing/malware attempts and the need to report hacking attempts.
- Ensure that home devices and networks are adequately protected, with clear advice on which anti-virus and email-filter software employees may install if required, and via implementing multi-factor authentication.
- Ensure that data that is required to be transported is also done so via protected mechanisms.
- Ensure that data is adequately backed up and capable of recovery and reconstitution.
- Test such back-up and recovery systems and test incident response plans.
- Log identified malicious attempts and alert employees with regular updates.

Whilst these present trying times do place stresses on the banking system, such basic steps may reduce risk and/or ensure that when claims arise they are met by (re)insurers in a speedy fashion. And whilst these are difficult times, banks should be looking to the future, re-appraising systems and preparing to do business again.

For more information please contact

JOHN BARLOW
Partner, Dubai
T +971 4 423 0547
E john.barlow@hfw.com

JUSTIN WHELAN
Partner, Abu Dhabi
T +971 2 235 4913
E justin.whelan@hfw.com

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our insurance and reinsurance capabilities, please visit hfw.com/Insurance-Reinsurance-Sectors.

hfw.com

Americas | Europe | Middle East | Asia Pacific