BCLP. Client Intelligent

Insights

NO PLACE LIKE HOME: HEIGHTENED RISKS FOR COMPANIES DUE TO COVID-19 AND REMOTE WORKING ARRANGEMENTS

Apr 22, 2021

SUMMARY

As the COVID-19 pandemic evolves so, too, does the threat of economic crime. Recent reports into fraud since the start of the pandemic highlight the extent of this threat but also confirm that the banking and finance industry has worked hard thus far to combat it. Many of the lifestyle changes caused by the pandemic look likely to stay for the long term. In this article we discuss the key types of economic crime posing the most risk to companies, particularly those in the financial services sector, and the steps that can be taken to mitigate these risks.

THE CURRENT CLIMATE

For its Global Economic Crime and Fraud Survey 2020[1], first published in March 2020, PwC surveyed 5,000 companies across 99 territories with striking results. 47% of respondents revealed that they had reported fraud in the previous 24 months, the highest figure in the history of the survey. The picture for UK companies is comparatively worse with 56% of respondents having reported fraud in the same period. Bear in mind that this was all before the pandemic hit.

The sharp increase in remote working triggered by COVID-19 has been a catalyst for record high cases of fraud and economic crime. Action Fraud reported a 400% increase in the number of fraud cases it received in March 2020 alone, as compared to February 2020. Over the course of the pandemic to date, Action Fraud estimates that £2.1 billion has been lost to fraudsters based on more than 350,000 cases of fraud that have been reported to it. These cases include reports of internal financial reporting fraud, market manipulation and insider trading, as well as fraud targeting individuals. We predicted that the pandemic would be the perfect storm for an increase in fraudulent activity. Given it is estimated that only 20% of frauds are ever reported,[2] we expect that Action Fraud's estimate is, sadly, only the tip of the iceberg.

Indeed, a report by UK Finance[3] published on 25 March 2021 unfortunately confirmed our prediction to be correct: payment industry fraud alone amounted to £2.83 billion in 2020. Whilst there was a decrease in the volume of certain types of fraud, such as invoice and mandate scams, there were some significant increases in the volume of others as compared to 2019. CEO Fraud (where the scammer manages to impersonate the CEO or other high ranking official of a victim's organisation to convince them to make an urgent payment to the scammer's account) increased by 24%, unauthorised remote banking fraud increased by 68% (including an increase in internet banking fraud of 117%), and authorised push payment fraud increased by 22%. UK Finance is one supporter of the Personal Investment Management & Financial Advice Association's call upon the Government[4]to include financial harm in the forthcoming Online Harms Bill.[5]We wait to see what will come of this but note that the Government's 2021 Budget only mentions tackling fraud within COVID-19 support packages.

The Royal United Services Institute for Defence and Security Studies ("RUSI") considers that the "prevailing political narrative fails to convey the full impact of fraud on the UK" and that "continued under-resourcing of the fraud response means that political rhetoric fails to match operational reality".[6]Given its pervasiveness and ability to undermine confidence in the rule of law, RUSI categorises fraud as an issue of national security. It has called upon the Government to facilitate improved intelligence architecture, provide a better resourced and coordinated policing response, and increase coordination with the private sector. Although the Government has not addressed the issue as of yet, regulators are certainly taking a more robust approach.

On 30 March 2021, the Crown Prosecution Service announced a new strategy to combat economic crime[7], having used figures from UK Finance and particularly commenting upon the fact that 86% of fraud reported during the pandemic has been cyber-enabled; in other words, remote working exacerbates the issue. Our team has written separately about the CPS' strategy.

EXTERNAL RISKS OF FRAUD

Typical techniques used to defraud victims, such as authorised push payment scams and hacking, remain commonplace and are being used against financial institutions and individuals alike.

In the case of Philipp v Barclays[8], Mrs Philipp and her husband, Dr Philipp, were approached by a fraudster who told them that he worked for the FCA and the NCA. He persuaded them to transfer Dr Philipp's savings into "safe accounts" in the UAE. In March 2018, Dr Philipp transferred £950,000 to Mrs Philipp's Barclays bank account. Mrs Philipp then transferred a total of £700,000 to two UAE accounts, all of which was stolen.

Mrs Philipps brought proceedings against Barclays alleging that the bank had breached its duty of care to her. The Court struck out her claim on the grounds that the Quincecare duty does not extend

to authorised push payments. The bank had no duty to protect Mrs Philipp from the consequences of her own decisions where, as between herself and the bank, her payment instructions were valid.

The Quincecare duty is now limited to cases where suspicions are raised, or ought to be raised, that there is a potential misappropriation of funds by a customer's agent i.e. a third party authorised by the customer. The Quincecare duty does not extend payments that have been expressly authorised by the customer themselves. In recognising this, the Court established that the duty of care owed to individual customers is more of a general adherence to safeguarding policies and procedures. This comes as welcome guidance on the limitations of a financial institution's liability but it is important not to become complacent. Simple though it may sound, the same tactics used against Mrs Phillips and her husband have been used very recently to defraud large financial institutions and companies as well, proving that it is not only overly trusting members of the public who may fall victim.

FINANCIAL CRIME RISKS INSIDE ORGANISATIONS

In addition to the external risk of fraud, the risk of financial crime committed within companies is very real for corporates and financial institutions, particularly whilst employees are working remotely.

With the increased difficulty in achieving financial targets and pressure to report attractive financial performance, financial reporting fraud is a significant risk. Similarly, for some employees, the temptation to exploit any weakness in surveillance so as to make money out of unusual market fluctuations will prove too much. Volatile markets and the accompanying surge in trading activity provide fertile ground for traders to amend marks without due respect to fair market value or to alter improperly their trading strategies. Note that there is precedent for this type of behaviour: both market abuse and internal financial reporting fraud rose during the 2000-2001 tech bubble and the 2007-2009 recession.

The FCA has made it clear that remote working cannot be used as a reason for lowering standards and has warned firms to exercise increased vigilance. Its updated COVID-19 guidance on firms' financial crime systems and controls,[9] and market trading and reporting,[10] indicates that it will be taking a more robust approach going forward in this respect. Further, the sympathetic approach previously adopted by the FCA to the operational challenges faced by firms coupled with the more flexible stance it took regarding client identity verification is no more; its statement supporting this approach expired[11]on 7 February 2021. Note, too, that the FCA announced on 12 January 2021 that it expects firms to ensure that all relevant communications (including voice calls) are recorded when working from home, which is a significant shift from its previous acceptance that firms may simply notify the FCA if recording was not possible on all occasions.

BEST PRACTICE

Regulatory scrutiny will be exercised with more vigour over the course of 2021 and beyond to combat the risks we have highlighted above. Although this may feel onerous to firms, the hope is that compliance with these stricter measures will protect companies from both internal and external risks posed by the unique working arrangements caused by the COVID-19 pandemic.

We encourage firms to continue to review and revise their approaches, as appropriate, to these threats by adopting Mathew Syed's 'Black Box Thinking'. Only by analysing lacunas, near misses or failures can procedures be adapted and risks continue to be mitigated.

1. Consider the process in place for applying information barriers and conflict lists. Have there been any near misses on recent transactions? Have conflicts been missed entirely and only checked after the event?

2. Can improvements be made to surveillance? Think about any lacunas. For example, surveillance can be improved by analysing the behaviour of the desks as a whole and individuals within them.

3. Is the risk assessment for fraud now out of date because it fails to consider COVID-19? Conducting a tailored fraud risk assessment for COVID-19 remote working and putting in place control measures as appropriate will strengthen companies' resilience to fraud attempts.

4. Do anti-corruption policies and employee training need refreshing?

5. Consider the procedure in place for internal investigations. Are there any lacunas in these procedures caused by the logistical restrictions of COVID-19?

While the world continues to adjust to long-term remote working, being cognisant of the seriousness of economic crime risks and adapting appropriately is the best way for individuals, companies and regulated firms alike to protect themselves from financial crime.

---

[1] https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

[2] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

[3] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021

[4] https://www.pimfa.co.uk/press-release/pimfa-calls-on-government-to-include-economic-harm-in-online-safety-bill-as-members-report-rise-in-increasingly-sophisticated-online-scams/

[5] https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

[6] https://static.rusi.org/the_silent_threat_web_version.pdf

[7] https://www.cps.gov.uk/cps/news/cps-launches-ambitious-plan-combat-economic-crime

[8] [2021] EWHC 10; https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Comm/2021/10.html&query=(Barclays)

[9] https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation

[10] https://www.fca.org.uk/firms/information-firms-coronavirus-COVID-19-response#market-trading-reporting

[11] https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation

RELATED CAPABILITIES

- White Collar
- Litigation & Dispute Resolution
- Financial Regulation Compliance & Investigations

MEET THE TEAM

Mukul Chawla KC

London

mukul.chawla@bclplaw.com
+44 (0) 20 3400 1000