TRAINING FOR ALL APPROPRIATE EMPLOYEES

JUL 2022

ManchesterCF
Financial Intelligence

The disruption caused by the COVID-19 pandemic is still being deeply felt around the world. The pandemic has had a damaging impact on the global economy with forecasts by economists that most major financial jurisdictions will have lost at least 3.4 percent of gross domestic product (GDP) in 2020[1]. Adding to concerns around the onset of a global recession are complications stemming from the ongoing Russia-Ukraine conflict and the fallout from sanctions.

Financial institutions are stuck in the crosshairs of all this turmoil. With institutional profit and ever-aggressive business-growth targets, allocating budgets and prioritising compliance training has long been considered a necessary, though underwhelming, operational expense. Many organisations prioritise marketing or public-relations budgets over compliance and training. Regardless, training mandates at financial institutions have evolved considerably since the Financial Action Task Force (FATF) first circulated its recommendations in the early 1990s. Terrorist acts around the world also put into sharp focus the vulnerabilities in the international financial system particularly where staff may be under-trained or unaware of basic red flags and typologies.

To protect the international financial sector, governments around the world have enacted legislation that requires financial institutions to provide ongoing employee training on financial crime risk. In the US, to comply with the Bank Secrecy Act (BSA), "[b]anks must provide training for appropriate personnel[2]." Perhaps in times past, the adjective "appropriate" has been interpreted by senior bank personnel to mean that training need only be given to a small cohort of compliance staff. Many compliance failings, civil actions and deferred prosecution agreements brought against global financial institutions in the past decade illustrate the fallacy of this logic. Thus, "appropriate personnel" includes the majority of bank employees from customer-facing staff to senior management[3]:

> *Training should be tailored to each individual's specific responsibilities, as appropriate. In addition, targeted training may be necessary for specific ML/TF and other illicit financial activity risks and requirements applicable to certain business lines or operational units, such as lending, trust services, foreign correspondent banking, and private banking.*

THE BENEFITS OF FINANCIAL CRIME TRAINING MAY COME IN THE FORM OF IDENTIFYING AND DISRUPTING HUMAN TRAFFICKING NETWORKS, RECOGNISING TYPOLOGIES RELATED TO WILDLIFE TRAFFICKING OR EXPOSING THE BUYING AND SELLING OF ART FOR SANCTIONS EVASION PURPOSES.

A number of stories have come to light in the past decade illustrating the benefits of financial crime training. These benefits may have come in the form of identifying and disrupting human trafficking networks, recognising typologies related to wildlife trafficking or exposing the buying and selling of art for sanctions evasion purposes.

It's likely that targeted training enabled financial investigators at Barclays Bank in London in 2016 to conduct an extensive investigation into business accounts it later determined to be shell companies created specifically for sanctions-evasion purposes. Arkady and Boris Rotenberg are Russian billionaires who were sanctioned by the US government in March 2014. To circumvent these restrictions, the Rotenbergs established offshore company with the help of Mark Omelnitski, a London-based attorney, through his company the Markom Group[4]:

> *Following the release of the Panama Papers in 2016, Barclays reviewed the companies formed by Mr. Omelnitski and the Markom Group. A Barclays internal investigatory memorandum concluded:*

> *Omelnitski and his company, Markom Group, created shell companies for sanctioned individual [Arkady] Rotenberg, a Russian oligarch, who is a close friend of the President of the Russian Federation, Vladimir Putin. Omelnitski is listed as a beneficial owner for the three companies owned by [Arkady] Rotenberg.* […]
>
> *The same Barclays memorandum noted, "[T]he ownership of these shell companies appears to be intentionally structured to be opaque in order to hide the identity of the true beneficiaries."*

WHEN FINANCIAL INSTITUTIONS DON'T SPOT (POSSIBLY DUE TO INADEQUATE EMPLOYEE TRAINING) OR FAIL TO ACT ON SANCTIONS VIOLATIONS, THERE ARE CONSEQUENCES.

Employees at Barclays clearly understood the potential risk of maintaining accounts for Omelnitski and his affiliated shell companies. By August 2017, all Markom Group accounts were closed.

When financial institutions don't spot (possibly due to inadequate employee training) or fail to act on sanctions violations, there are consequences:

- Between 2012 and 2014, the Bank of Tokyo-Mitsubishi UFJ (BTMU), now MUFG Bank, admitted to several sanctions and transaction monitoring missteps resulting in fines of over USD570m[5].
- In July 2014 BNP Paribas was fined USD8.9 billion, had its US-dollar clearing licence revoked, was forced to fire senior executives and was also required to appoint an independent monitor[6].
- In March 2015, a six-month-long investigation of Commerzbank culminated in a USD1.45-billion penalty for sanctions breaches[7].

The consequences of bank personnel undervaluing or failing to prioritise ongoing employee training goes well beyond fines and currency clearing restrictions. The fallout from failing to provide appropriate training to all appropriate employees (ie, most of the staff) can also result in reputational damage. The 2022 case brought against USAA FSB by the Office of the Comptroller of the Currency (OCC) and the Financial Crimes Enforcement Network (FinCEN) for failure to meet commitments to improve its anti-money laundering (AML) program is an example of what can happen when bank staff are undertrained for their roles[8]:

THE FALLOUT FROM FAILING TO PROVIDE APPROPRIATE TRAINING TO ALL APPROPRIATE EMPLOYEES (IE, MOST OF THE STAFF) CAN RESULT IN REPUTATIONAL DAMAGE.

> *Management did not tailor USAA FSB's training program for the FIU investigators (including third-party contractors) and* [know your customer (KYC)] *analysts to the Bank's risk profile and suspicious activity typologies. For example, training in 2020 focused on changes in policies and procedures and the documentation of certain reviews in the Bank's systems, but failed to address how to analyze accounts or to describe what constitutes potential suspicious activity.*

One particular example explored in the consent order involved Customer B. In 2019, Customer B's USAA FSB account[9]

> *alerted on indicators of possible suspicious activity, and the Bank reviewed the alert. The Bank closed initial reviews of alerted activity without escalation and without a thorough review of the customer's reported source of income and the counterparties involved. However, the underlying activity within the account showed significant red flags, including receiving payments for what may have been unlawful internationally-based prostitution/escort ventures.*

The red flags such as those referred to in this instance, are often also used to identify potential human traffi king cases, but were not reported as suspicious in a timely manner by USAA FSB. Further, finding related to this specific case show that[10]

> [o]*ver a one-month period, Customer B received three wire transfers from an individual located overseas totaling $44,500. These transfers referenced "art purchase," but there was no discernable, legitimate connection between Customer B and the art industry. Additionally, further investigation connected the foreign-based individual to an offshore entity named in*

the Panama Papers. From May 10, 2019 through June 29, 2020, Customer B engaged in approximately $125,000 of suspicious activity. USAA FSB did not report this activity to FinCEN until July 22, 2020 – over one year later.

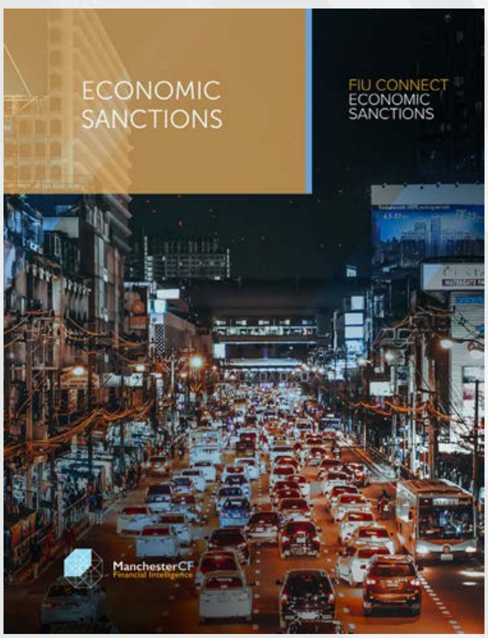
The OCC and FinCEN case brought against USAA FSB did result in a fine of USD140m. However, the consent order also seems to be making a point beyond instituting a monetary penalty.

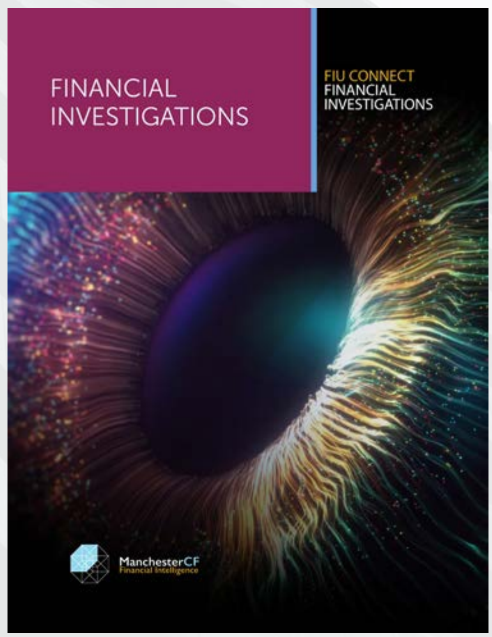
When training programs are poorly constructed and inadequate, it signals to regulators, and potentially the wider public, that the financial institution is indifferent to protecting the global financial system or victims of financial crime.

That's not a great image for a bank to have. Consider the budgets many international financial institutions put into public-relations campaigns.

> WHEN TRAINING PROGRAMS ARE POORLY CONSTRUCTED AND INADEQUATE, IT SIGNALS TO REGULATORS, AND POTENTIALLY THE WIDER PUBLIC, THAT THE FINANCIAL INSTITUTION IS INDIFFERENT TO PROTECTING THE GLOBAL FINANCIAL SYSTEM OR VICTIMS OF FINANCIAL CRIME.

Imagine if a small portion of that budget were to be redirected to augment staff training. Not only would the financial institution's reputation be improved, but there would be a less likelihood of financial loss through fines or other penalties. From an economic perspective, providing training to employees in all lines of business just makes business sense.





[1] https://www.statista.com/topics/6139/covid-19-impact-on-the-global-economy/#topicHeader__wrapper

[2] https://bsaaml.ffiec.g v/manual/AssessingTheBSAAMLComplianceProgram/05

[3] Ibid.

[4] *The Art Industry and US Policies that Undermine Sanctions*, United States Senate, Permanent Sub-Committee on Investigations, July 2020; Barclays Internal Memorandum (BARC006752–61).

[5] "The Bank of Tokyo Mitsubishi-UFJ, Ltd., New York Branch," Consent Order Under New York Banking Law § 39 and 44, New York State Department of Financial Services, November 18th 2014.

[6] https://www.dfs.ny.gov/search/site?search=bnp+paribas

[7] Consent Order in the Matter of Commerzbank AG, NYDFS, March 11th 2015; "NYDFS announces Commerzbank to pay $1.45 billion, terminate employees, install independent monitor for banking law violations", NYDFS press release, March 12th 2015.

[8] https://www.fincen.g v/sites/default/files/enfo cement_action/2022-03-18/USAA%20Consent%20Order_Final%20508%20%282%29.pdf

[9] Ibid.

[10] Ibid.