مصرف لبنان
BANQUE DU LIBAN

Combating Banking Fraud and Banque Du Liban's Initivaties

Raed H. Charafeddine, First Vice-Governor, Banque Du Liban

Association of Certified Fraud Examiners Lebanon Chapter
2nd Annual Fraud Conference
February 8, 2018 | Beirut - Lebanon

Table of Contents

I. Introduction

Ladies and Gentlemen,

I would like to thank the Lebanon chapter of the ACFE for their kind invitation to address such a critical topic, which is fraud, from the financial-banking perspective that touches vital socioeconomic interests.

When Charles Ponzi witnessed the collapse of his fraudulent scheme in the 1920s, which became the infamous Ponzi Scheme, luring millions of people into his money-making "investment" and causing losses for his investors which reached $20 million (around $240 million today), it was beyond his wildest imagination that his record would be topped by far through a similar scheme almost nine decades later by Bernard Madoff in 2008, which cost investors roughly $18 billion.[i] This recurrence simply proves that fraud is not only a time lasting and adaptive phenomenon, but also an escalating and invasive one.

In what follows, I will shed some light on some significant aspects of fraud in general and banking fraud in specific, as to figures, sources, and controls. Next, I will address the major critical challenges that face the financial-banking sector in combating fraud, and finally I will briefly state Banque Du Liban's most important endeavors in setting an anti-fraud corporate governance culture.

II. Fraud: Figures, Sources, and Controls

A. Figures

Fraud's varied scope of action and influence has intensified its damages and diversified its risks to strike at nearly every economic dimension, as economies and firms struggle to recover from the global financial crisis and its consequent stagnation. According to the ACFE estimates, the typical organization loses 5% of annual revenues to fraud, whereby global total loss exceeded $6.3 billion in 2016[ii], the Middle East and North Africa region recording the highest level of median losses worldwide of $275,000. Of the three major categories of occupational fraud, financial statement fraud caused by far the greatest median loss per scheme, the other two being asset misappropriation and corruption[iii].

On the level of banking and financial services, frequency of fraud schemes in victim organizations recorded its highest levels in the categories of corruption (38%) and cash-related fraud (29%), indicating the critical importance of internal control and scrutiny for combating fraud in such a sector[iv]. Moreover, banking and financial services have, by far, the highest incidence of fraud, accounting for 17.8% of cases in 2016 compared with 10.3% for the next highest category, government and public administration[v], with a median loss of $192,000 per case, whereas 2015 witnessed more complex schemes at which 23% of fraud cases caused losses of $1 million or more each[vi]. According to the ACFE, fraud cost the banking industry $67 billion per annum in 2014, of which 70% was internal, and most remains undetected[vii].

B. Sources

Sources of banking fraud are divided into internal and external categories. Internal fraud largely can result from front-office/back-office user behavior or privileged IT admin activities. Broadly, external frauds reported by banks can be divided into three main sub-groups: technology related, KYC related (mainly in deposit accounts), and advances related (loan portfolio). Reported fraud cases have revealed that around 65% of the total fraud cases were technology related frauds (covering frauds committed through/at internet banking channel, ATMs, and other alternate payment channels like credit/debit/prepaid cards) while the advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds.[viii]

C. Controls

Traditionally, external audits of the financial statements, code of conduct, and management certification of the financial statements were consistently among the most commonly implemented controls across organizations in all locations. According to an ACFE study, active detection methods, such as surveillance and monitoring or account reconciliation, proved to be more effective than traditional passive methods. Moreover, the most prominent organizational weakness that contributed to the frauds was a lack of internal controls and an override of existing internal controls.[ix]

IT complexity cited as the top risk factor that organizations face, employees with the highest levels of access to IT systems, such as systems and database administrators, are perceived to be potential perpetrators who commit or facilitate fraud. Furthermore, new channels such as online banking, mobile banking, and social networks only add to the complexity of combating fraud, hampered by legacy systems that make IT security hard to monitor. In this context, 30% of financial services companies have been affected by data theft – the most common form of fraud within the industry. Complicating the scene even further, fear of bad publicity and the cost and time of investigation are the most frequently cited reasons why cases of fraud are not referred to criminal prosecution. Data theft and internal financial fraud both affected about 30% of financial services companies, regulatory and compliance breaches occurred in 26%, and money laundering in 8%[x] of them.

Based on the aforementioned, instating active methods of prevention and detection, avoiding risks of external breaches, and enhancing internal controls all require a mix of "old school" procedures and layers of technology[xi]. Acknowledging the importance of traditional prevention and detection methods, such as external audits, code of conduct, management certification of the financial statements, and whistleblowing, cutting-edge technologies have proven to be essential for coping with contemporary fraud risks. These technologies encompass such techniques as continuous oversight of IT platforms, big data analytics, real time processing, and profiling[xii]. As a matter of fact, fraud prevention is becoming more possible with the emergence of artificial intelligence. Hence, risk management, audit, and compliance practices are able to foresee fraudulent risks in a comprehensive manner, thus encompassing preventive feedforward control, detective concurrent control, and feedback control.

III. Critical Challenges in Combating Fraud

The impact of frauds on financial services institutions, such as banks, is more significant as their operations involve intermediation of funds. The economic cost of frauds can be huge in terms of market failures, endangering financial stability, and disrupting the payment system. Besides, frauds can have a potentially devastating effect on confidence in the banking system, the integrity and stability of the economy, the central bank's supervisory role, and even create social unrest, discontent, and political upheavals. The vulnerability of banks to fraud has been heightened by modern technological advancements[xiii]. Such risks inflict critical challenges, the most prominent of which are the following:

- Utilizing optimal technologies and best practices in the race battle between financial services institutions and fraudsters;[xiv]
- Setting a multi-factor authentication/multi-layered security structure;[xv]
- Raising fraud awareness through continuous education of financial consumers;[xvi]
- Incorporating vigorous corporate governance standards;
- Exchanging of information between all stakeholders to instill and maintain financial discipline;[xvii]
- Maintaining close liaison with investigating agencies and courts to ensure timely completion of investigations and closure of cases;[xviii]
- Conducting data analysis that provides an effective way to be more proactive in the fight against fraud;[xix]
- Enhancing the skills for fraud examiners, particularly technological and IT skills, versatile work experience, strong corporate background, and international capabilities;[xx]
- Combating fraud through a top-bottom approach reinforced by senior management;[xxi]
- Creating a no-opportunity culture that breaks down the fraud triangle of "pressure, opportunity, and rationalization"[xxii] through conducting an annual fraud risk assessment[xxiii] and audit plan[xxiv].

IV. Banque Du Liban's Anti-Fraud Governance

Despite Lebanon's international rating in regards to its retarding record in corruption and social trust, Banque Du Liban has been persistent to play an exemplary regulatory role in establishing a robust, well-regulated, and compliant Lebanese financial system, which has proved to be a role model in preserving national financial integrity on the regional and international levels. This model is established on a deep-rooted anti-fraud governance satructure that is based on active techniques of fraud prevention and detection, modern technology, diligent surveillance and monitoring, and rigorous internal control requirements. BDL's anti-fraud model encompasses the following pillars:

First, payment system. BDL plays a key role in the development of domestic payment systems. It has regulated e-banking to provide a secure platform for

e-services in the Lebanese financial sector, stressing compliance with international norms and standards in order to promote safety and improve efficiency of the multi-currency payment system in Lebanon. In order to enhance economic efficiency, BDL has adopted real time online connections with the financial sector through implementing the Real Time Gross Settlement (RTGS) system for domestic settlement, offering the banking and financial sectors a secure, reliable and real time method of payment that adheres to international standards. Moreover, BDL has set in place the automated Retail Payment and Clearing System (BDL-CLEAR), a low value - high volume bulk payments system, for clearing retail payments, including cheques, direct debits, and card transactions.

Second, risk management. BDL has strived to protect the financial-banking sector and preserve its reputation by reinforcing measures pertaining to anti-money-laundering and combating-the-financing-of-terrorism, cross-border transportation of cash, tax evasion, and international sanctions. Accordingly, BDL required that banks establish Risk Committees to oversee risk management implementation, and it requested from banks and financial institutions to establish Legal Compliance Units that are in charge of identifying and preventing legal risks. Furthermore, BDL established the Financial Stability Unit and the Compliance Unit to monitor the stability and compliance of the financial sector.

Third, corporate governance. Being aware of the importance of corporate governance in optimizing the performance of the financial sector and protecting the interests of its stakeholders, BDL emphasizes compliance with the principles of good governance at all banking and financial managerial levels, including boards of directors and senior management. This is done in parallel with the creation of appropriate awareness in financial institutions, whereby compliance units were established to protect the banks. This approach aims at increasing transparency and enhancing prudent management as main objectives of BDL policy, which has established for this purpose the Unit of Corporate Governance.

Fourth, internal audit. Banque du Liban has instructed banks to establish an internal control framework that is appropriate to the size of the bank or financial institution and to the nature of the risks faced or to be faced by them. Banks and financial institutions were also required to establish an "Internal Audit Unit" to oversee the work of the bank or financial institution.

Fifth, career competence and effectiveness. BDL imposed academic, technical, and ethical requirements for staff in key banking and financial positions, in addition to requiring the documentation of a succession plan.

Sixth, consumer protection. BDL has required that banks establish consumer protection units to ensure that they deal fairly with all their customers in a transparent manner, and it enhanced financial education to enable customers protect their rights through conducting training programs for student internship and public teaching, and disseminating information through pamphlets, workshops, awareness campaigns, conferences, speeches, and interviews. In line with this, BDL established the Consumer Protection Unit at the Banking Control Commission to ensure the compliance of banks.

V. Conclusion

I would like to conclude with an expressive quote for the American writer James Surowiecki, which says: "the challenge for capitalism is that the things that breed trust also breed the environment for fraud". This could be, to large extent, true; however, it is also true that our mission is to breed a culture of integrity on the debris of fraud.

Thank you.

References

[i] http://www.telegraph.co.uk/business/2016/04/13/bad-for-business-ten-notorious-corporate-scandals/charles-ponzis-schemeyear-1920losses-20m-at-the-timethe-infamous/

[ii] http://www.acfe.com/rttn2016/about/executive-summary.aspx

[iii] *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study*, The Association of Certified Fraud Examiners.

[iv] http://www.acfe.com/rttn2016/victims/organizations.aspx

[v] *A-Z of Banking Fraud 2016: the What, Why and How*. Temenos and NetGuardians, 2016.

[vi] *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study.*

[vii] *A-Z of Banking Fraud 2016: the What, Why and How.*

[viii] Chakrabarty, K., 2013. *Fraud in the Banking Sector: Causes, Concerns and Cures.* ASSOCHAM, 2013.

[ix] http://www.acfe.com/rttn2016/about/executive-summary.aspx

[x] *A-Z of Banking Fraud 2016: the What, Why and How.*

[xi] https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534

[xii] *A-Z of Banking Fraud 2016: the What, Why and How.*

[xiii] Chakrabarty, K., 2013.

[xiv] *A-Z of Banking Fraud 2016: the What, Why and How.*

[xv] https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534

[xvi] Ibid.

[xvii] Chakrabarty, K., 2013.

[xviii] Ibid.

[xix] *Fraud Detection Using Data Analytics in the Banking Industry*. Discussion whitepaper, acl, 2014.

[xx] https://www.bankinfosecurity.com/5-must-have-skills-for-fraud-examiners-a-3847

[xxi] http://cdn2.hubspot.net/hubfs/556947/PDF_Downloads/Fraud_White_Paper.pdf?submissionGuid=df10deac-d550-4c76-8eea-42071bfa15b2

[xxii] http://www.dkcpas.com/content/client/7fa6b31cca001f1ab32e5d2a03a5b153/uploads/iconic-fraud-triangl.pdf

[xxiii] Ibid.

[xxiv] Goldmann, P., 2010. *Financial Services Anti-Fraud Risk and Control Workbook*. John Wiley & Sons, Inc., Hoboken, New Jersey.