DOI https://doi.org/10.30525/2592-8813-2024-spec-17

PROBLEMS OF MODERN BANKING COMPLIANCE

Andrejs Surmačs,
Baltic International Academy, Latvia
ansuinvest@gmail.com

Evelina Surmača,
Royal Holloway University of London, England
Business and Management
evelina.surmach@icloud.com

Abstract. The enforcement of modern compliance in EU commercial banks has identified several issues. However, the issue of concern is that commercial banks were aggressively charged heavy penalties by supervisory authorities, as well as the removal of board members and revocation of licences from commercial banks. The second issue of concern is reasonable doubts about how the banks enforce the bank secrecy principle. The authors of the article analyse the issues of modern banking compliance and propose ways to solve the issue of compliance requirements by bank customers especially commercial banks while maintaining the principle of non-disclosure of bank secrecy.

The relevance and novelty of the topic are indisputable. Problems of modern compliance affect the interests of all participants in the current financial market.

The purpose of the study is to identify and eliminate problems in the enforcement of effective compliance that suits all parties while maintaining the principle of bank secrecy.

Key words: compliance, banks, bank secrecy.

Introduction. Compliance issues became relevant for the modern banking market already in 2001. Following the terrorist attacks in the United States on 11 September 2001, the entire banking world changed dramatically [1]. Governments of all democratic countries have begun to introduce the comprehensive concept of "Know Your Customer" policies into the banking sector. Requirements from banking sector supervisory authorities have become a pressing issue for banks, their customers and the supervisory authorities alike. Over time, the requirements of the "Know Your Customer" policy were constantly tightened, which ultimately resulted in heavy penalties imposed by supervisory authorities on the players in the banking sector, dismissal of board members, and revocation of licences from commercial banks. Issues of maintaining banking secrecy most urgently appeared on the agenda.

The authors of the study set themselves the goal of identifying problems concerning compliance, finding ways to solve them and elaborating specific proposals to eliminate these problems.

The success was achieved in substantially meeting the objectives set in this study by applying the historical reflection and deduction techniques.

The authors conducted a historical study of the development of banking compliance, identified problem aspects in the enforcement of the "Know Your Customer" policy in the banking sector, summarised all the identified problems accumulated in banking compliance since 2001, and addressed the challenges identified.

Basic theoretical and practical provision. The compliance legislation originated in the United States. The US Foreign Corrupt Practices Act (FCPA), which came into force in 1977 was first elaborated and adopted.

However, the initial starting point for the introduction of banking compliance should be considered the date of 11 September 2001. On this day, America declared war on international terrorism and began to implement legal acts in international banking compliance [1].

It is essential to bear in mind that before 11 September 2001, there was no compliance in the global banking sector. Prior to11 September 2001, banks generally did not inquire about the source of origin of customer assets. They were not particularly interested what type of business activities their customers and beneficiaries of the companies were conducting. At this time, commercial banks fully complied with the principles of banking secrecy. In many credit institutions, it was possible to create an account using a code word without presenting a passport or identifying the customer.

Banking supervisory authorities and Central Banks did not impose compliance requirements on commercial banks. Even though in some countries in the early 2000s laws were passed on "Prevention of money laundering and terrorist financing", the requirements of these laws were not fulfilled in practice [2].

Since 2002, the requirements introduced by supervisory authorities to commercial banks worldwide have been constantly growing. New laws were adopted to prevent the laundering of assets obtained by criminal means. The requirements of old laws were clarified and have become stricter. By 2002, reasonable and justified requirements for customer identification when creating a bank account appeared. There were introduced bans on coded accounts. The first requirements for the implementation of the "Know Your Customer" policy began to appear and be implemented. They were general and there were no instructions for their implementation from the supervisory authorities. Bank customers did not want to disclose any information about their business. Banks, in turn, did not want to disturb their customers, understanding that the market is highly competitive, and customers can take the business to another bank where they are not obliged to answer any "tough" questions. Commercial banks tried to comply with the new requirements of supervisory authorities by searching for information from external sources and the Internet.

At this time, compliance departments were formed in commercial banks. The employees were appointed among customer managers who, in friendly conversations with customers, tried to find out the information necessary to fulfil the requirements of the law and supervisory authorities.

Inspections of banking supervision by central banks in 2003 revealed shortcomings in the policies and procedures of commercial banks. Commercial banks receive instructions to improve the requirements for implementing compliance policies.

By 2005, a new term was introduced in the banking sector: "Beneficiary of assets". Financial institutions are required to know the true owners of all assets held in a commercial bank. At this time, the requirements of the "Know Your Customer" policy continue to become more stringent. Information about the customer from open sources is already considered insufficient. Banks are required to introduce questionnaires in which customers must personally indicate information about the origin of their assets and complete information about their business. Banks, at this time, commenced random requests to present respective agreements on the economic activities of their customers.

Banking supervision audits carried out by central banks by 2006 continued to identify deficiencies in the policies and procedures of commercial banks. Commercial banks are receiving orders to improve the requirements for implementing compliance policies and laws on preventing money laundering and terrorist financing [3].

The concept of responsibility of individual members of the bank's board of directors responsible for compliance in the bank is introduced. At the legislative level, penalties are introduced for non-compliance with compliance regulations.

In 2010, banks commenced the execution of automated compliance systems for all banking operations. The number of employees in the compliance departments of commercial banks exceeds the number of employees in the legal departments of banks. Compliance employees are prohibited from communicating directly with the customer. The very essence of a compliance officer role is changing. These are specially trained professionals who have nothing in common with the customer managers who began working in these departments in 2002. The compliance officers were mainly responsible

for finding information compromising the customer to identify and prevent reputational risks for a commercial bank.

Moreover, banks began to request legal documents from customers for virtually all transactions at that time. This made customers very nervous. The contracts contain secret information, the leakage of which to competitors can lead to large financial losses. However, customers, under threat of account closure, are forced to provide the required information to banks. It is becoming difficult to create accounts in other banks. Banks exchange information about closed accounts with each other. The first cases appear when newly formed companies do not pass compliance checks in commercial banks and thus cannot create operating accounts in any bank at all [4, 5].

Banking supervision audits carried out by central banks by 2011 continue to identify shortcomings in the policies and procedures carried out in commercial banks. Commercial banks are being instructed to improve the requirements for establishing and adopting compliance policies and laws on preventing money laundering and terrorist financing. A large framework of problems appears. A matter of concern is that supervisory authorities annually increase the requirements for commercial banks in compliance, whereas banks do not understand what new requirements will be imposed on them by supervisory authorities [6, 7].

At this time, supervisory authorities, due to improper compliance requirements on the part of commercial banks, began to heavily charge penalties from banks. The first board members of commercial banks responsible for compliance issues appear to be suspended.

By 2015, banks are beginning to purchase automated banking software designed to track all customer transactions and identify compliance risks. From now on, banks require their customers to justify all transactions concluded by customers. The presence of contracts, invoices and other initial information is not considered sufficient. It is necessary to convince the bank that the transaction being concluded was cost-effective for all parties to the transaction and that the transaction price is market price. This had to be confirmed with estimates, quotes and other reliable information.

Banking supervision audits by central banks by 2017 continue to identify shortcomings in the policies and procedures of commercial banks. Commercial banks are being instructed to improve the requirements for implementing compliance policies and laws on preventing money laundering and terrorist financing. At this time, the first precedents appeared for the removal of supervision of all members of the Board of Directors of individual commercial banks. Members of the Bank Councils receive warnings about dismissal from their positions if there is no improvement in the compliance activities of a commercial bank. From the supervisory side, the first signals are appearing regarding the possible revocation of a commercial bank's licence due to improper compliance with the requirements of the "Know Your Customer" policy [8, 9].

By 2023, banks in the European Union and worldwide have introduced general compliance requirements that every participant in the financial sector must comply with [10]. These include the requirements for identifying the customer and the beneficiaries of the assets, a complete understanding of the customer's business and the transactions it enters, and a complete understanding of the economic essence of each operation of a commercial bank and its customers. Bank customers are not allowed to directly communicate with compliance department employees. All communication with the bank occurs through customer managers. Banks are implementing multimillion-dollar software, an artificial intelligence-powered product, to combat the laundering of criminally obtained assets. It is not uncommon that customer assets are not debited according to the customer's payment order until acceptance has been received from the bank compliance officer. Commercial banks request information from each other about customers and their assets and actively share this information. Having a customer undergo compliance procedures in one bank does not mean that there are no questions for the customer from the compliance department of another commercial bank.

At the same time, banking supervision audits continue to identify shortcomings in the policies and procedures of commercial banks. Commercial banks continue to receive instructions to improve the requirements for implementing compliance policies. Commercial banks are facing multimillion-dollar penalties for failing to adequately comply with anti-money laundering laws. Due to insufficient compliance with the requirements of laws on the prevention of money laundering, licences of commercial banks are revoked [11].

The problems of commercial banks experience with compliance highlighted not only the problems of banks with supervisory authorities, but also deep problems with bank customers. If earlier they tried to understand the attitude of banks in the field of "Know Your Customer" policy, then at this stage they refuse to rationally perceive the actions of commercial banks in the field of compliance. The fear of losing an operating account leads to submissive and powerless compliance with the requirements of commercial banks. At the same time, largest customers of commercial banks are faced with a new problem – maintaining trade secrets.

According to the dictionary and laws on bank secrecy: "Banking secrecy is a legally guaranteed principle of banking activity, according to which banks and other credit institutions undertake not to disclose information about their customers and to keep confidential all data on transactions carried out for respondents without exception"[12].

"Industrial espionage is a form of unfair competition in which the illegal receipt, use, disclosure of information constituting a commercial, official or other secret protected by law are carried out to obtain advantages in carrying out business activities, as well as obtaining material benefits" [13].

The main purpose of industrial espionage is to save money and time to enter new markets for the enterprise.

The concept of industrial espionage includes obtaining information about counterparties, obtaining information about the volume of transactions, obtaining information about the price of goods or services, obtaining information about discounts and other privileges, financial information about the success of a business, reporting, information about managers, other information [13].

All the above information, according to the latest compliance requirements, must be submitted by customers to a commercial bank.

Access to this information is available to bank employees, employees of supervisory authorities, employees of all correspondent banks, police officers, tax authorities, prosecutors and many others.

Research findings or data, evaluation of research results. Based on the analysis, the authors of the study identify two unresolved problems:

1) Commercial banks cannot predict and timely fulfil the ever-increasing requirements of supervisory authorities concerning bank compliance monitoring. Supervisory authorities, for their part, are constantly increasing the requirements for compliance in banks. Now, there are no regulatory documents that set out the requirements and criteria for mandatory execution by commercial banks. Banks do not know and cannot independently determine where the boundaries of "sufficient" compliance are. Nevertheless, commercial banks, not wanting to spoil relations with supervisory authorities, prefer to pay heavy penalties, risk their licence and continue to work.

2) The second unresolved problem is related to the fact that with the introduction of modern compliance, commercial banks became the owners of all the commercial information of their customers.

Previously, to commit industrial espionage, it was necessary to infiltrate one's people into a competitor's company. It was not, however, an easy task and obtaining extensive information was difficult. Today, it is enough to enter a conspiratorial alliance with any employee of the compliance department of a commercial bank, where a competitor's company has created an operating account, and all the necessary information will be available. The owners of this information are bank compliance officers, bank management, bank tellers, bank customer managers, bank internal audit staff, bank external audit staff, supervisory staff, police, prosecutors and many others.

Conclusions. Considering the foregoing, the authors of the study draw the following conclusions:

1) The requirements of supervisory authorities for commercial banks are neither systematised nor reflected in regulatory documents. This leads to the fact that commercial banks are unable to understand the scope of necessary measures when implementing compliance policies, which results in constant sanctions imposed by supervisory authorities upon commercial banks.

2) The volume of information requested from customers by commercial banks and its further dissemination inside and outside the bank leads to well-founded fears of possible illegal access to this information by third parties.

To solve these problems, the study authors make the following suggestions and recommendations:

3) The supervisory authorities for commercial banks of the European Union, represented by the European Central Bank, must issue a regulatory document that clearly describes:

– a sufficient level of information requested from customers;

– procedures for processing this information;

– procedures for accessing and storing this information.

4) The supervisory authorities for commercial banks of the European Union, represented by the European Central Bank, must develop and implement unified software for processing information received from customers to identify potential risks and terminate cooperation with unreliable customers. The implementation of compliance procedures in one bank of the European Union must be complete, sufficient and acceptable for other banks in the European Union.

5) At the level of the European Union, it is necessary to develop and implement effective legislative regulations within the area of responsibility of all persons who have access to confidential information stored in commercial banks.

References:

1. Miller center UVA, Timeline: The september 11 terrorist attacks. (2001). Retrieved from: https://millercenter.org/remembering-september-11/september-11-terrorist-attacks
2. Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums. LR.,(2006). Retrieved from: https://www.d-k.lv/rus/documents/laws/689/710/
3. A.Schilder: Banks and the compliance challenge. (2006). Retrieved from: https://www.bis.org/review/r060322d.pdf
4. FKTK jāvērtē iemesli banku attekumam atvērt norēķinu kontus NVO. LSM.LV. (2023). Retrieved from: https://www.lsm.lv/raksts/zinas/ekonomika/fktk-javerte-iemesli-banku-atteikumam-atvert-norekinu-kontus-nvo.a385525/
5. J.Stukāns: Par kontu neatvēršanu NVO bankas jāsoda. Neatkarīgā. (2020). Retrieved from: https://neatkariga.nra.lv/izpete/333630-juris-stukans-par-kontu-neatversanu-nvo-bankas-jasoda
6. Compliance with the AML/CFT International Standart. IMF, (2011). Retrieved from: https://www.imf.org/external/pubs/ft/wp/2011/wp11177.pdf
7. What Are Banks Spending on Compliance? Bankers as Buyers 2011. AFAC. (2011). Retrieved from: https://compliance.docutech.com/2011/02/03/what-are-banks-spending-on-compliance-bankers-as-buyers-2011/
8. FKTK piemēro sodu "PrivatBank" valdes locekļiem. NRA. (2015). Retrieved from: https://nra.lv/ekonomika/latvija/158131-fktk-piemero-sodu-privatbank-valdes-locekliem.htm
9. Moldovas gadsimta zādzība: "PrivatBank" piemērots 2 miljonu eiro sods un atstādināta vadība. DB. (2015). Retrieved from: https://www.delfi.lv/bizness/37293360/bankas_un_finanses/46828889/moldovas-gadsimta-zadziba-privatbank-piemerots-2-miljonu-eiro-sods-un-atstadinata-vadiba
10. Compliance to play large role in banking-as-a-service sector in 2023. S&P Global. (2023). Retrieved from: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/compliance-to-play-large-role-in-banking-as-a-service-sector-in-2023-72822966

11. Neatbildēts jautājums ABLV Bank lieta: kāpēc prokuratūra vēlējās slēgtas tiesas sēdes? LA.LV. (2023). Retrieved from: https://www.la.lv/neatbildets-jautajums-ablv-bank-lieta-kapec-prokuratura-velejas-slegtas-tiesas-sedes
12. Банковская тайна. (2023). Retrieved from: https://www.google.com/search?q=%D0%B1%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2%D1%81%D0%BA%D0%B0%D1%8F+%D1%82%D0%B0%D0%B9%D0%BD%D0%B0
13. Промышленный шпионаж. Википедия. (2023). Retrieved from: https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%88%D0%BF%D0%B8%D0%BE%D0%BD%D0%B0%D0%B614.