CHAPTER 7

CHAPTER 7

BANKING SUPERVISION DEPARTMENT ACTIVITY

In 2022, the Banking Supervision Department focused on improving the banking system's ability to withstand an economic crisis and on strengthening its resilience. It also continued to strengthen the bargaining power of households and improve competition in the banking system. In view of these effects, a number of reforms were promoted that will benefit the banking system's customers and they are described in detail in this chapter.

1. THE BANKING SUPERVISION DEPARTMENT'S VISION AND STRATEGIC GOALS

The Banking Supervision Department's vision is "to provide professional and proactive supervision that will benefit the public and the economy." The Banking Supervision Department's goals are derived from the language of the law and from the strategic goals adopted to support the achievement of that vision. The law specifies that the Banking Supervision Department will work on behalf of the public and the economy by means of three main objectives: preserving the ability of the banking corporations to fulfill their commitments; ensuring the normal functioning of the banking corporations and protecting the interests of their customers; and supporting the stability of the financial system.

The Banking Supervision Department's strategic goals are in line with those of the Bank of Israel:

- Stability—Protecting the funds of depositors; weathering crises; ensuring the continuity of services to the public both in an emergency and in normal times;
- Fairness—Assimilating a culture of fairness toward customers that is inclusive and impactful.

The following are its secondary objectives:

- Creating a more competitive and advanced financial system for the benefit of its customers;
- Adaptation of the Banking Supervision Department's operating model to a changing environment.

2. THE MAIN ACTIVITIES TO STRENGTHEN STABILITY AND PROTECT THE FUNDS OF THE BANKS' DEPOSITORS

The Banking Supervision Department's goal is to strengthen the stability of the banking system and to ensure its normal functioning in the following areas:

The macro environment—the assessment of risk

As a result of the increase in risk in the macroeconomic environment, due to, among other things, the increase in inflation and interest rates worldwide, the volatility in the financial market and the lack of geopolitical stability, the Banking Supervision Department has worked to ensure that the banks' preparedness for changes in the economic environment are monitored and managed by the banks' boards of directors and executives and that the financial indices (capital adequacy, liquidity and profitability) are stable and in line with observed risks. There have recently been a number of bank collapses worldwide, in which it appears that the aforementioned developments were at the root of the problem. The Banking Supervision Department is aware of the danger that the domestic banks will be infected and is working to learn the lessons of those developments.

A survey of the mortgage market

During the past year, the Banking Supervision Department carried out a survey of the market for housing credit. The survey included a comprehensive quantitative analysis of the housing market and the mortgage market and an examination of the most important indices of risk, with emphasis on repayment ability. The survey looked at the increased appetite for risk in the banking system, which was reflected in the increase in its scope of activity and in its proximity to regulatory limits. The survey also examined the steps taken by the banks as a result of recent changes in macro conditions (the increase in interest rates and inflation and various scenarios), with special attention devoted to sensitivity tests and stress tests carried out by the banks (in addition to the Banking Supervision Department's stress test). The survey produced some important findings, which were discussed in detail with each of the banks.

The effect of the increase in interest rates on mortgage payments

In parallel to an analysis of the detailed data possessed by the Banking Supervision Department on the effect of the increase in interest rates on mortgage payments, the Banking Supervision Department examined which focal points of risk each of the banks identified in its environment and, together with the banks, examined the solution they are offering to their customers in this context. The findings indicate that mortgage payments have increased considerably, primarily among customers who took out mortgages during the last 18 months, although they enjoy a relatively high income and so far there has not been any degradation in the quality of the banks' credit portfolio or any major increase in arrears. Similarly, the investigation indicated that the banks allow their customers to spread out payments on the Prime rate track, without any additional cost, for relatively long periods and that they carry on a dialogue with customers who may have trouble in making their mortgage payments (see Box 5.2).

Strengthening the level of cyber security in the banking system

The Banking Supervision Department continued its activities this year to improve and strengthen the banking system's level of cyber security. In this context, a long-term plan to upgrade the financial CERT[1] (which provides a response to specific threats facing the financial sector) was approved by the Governor of the Bank of Israel, the Supervisor of Banks, and financial regulatory entities, as well as senior officials in the National Cyber Directorate and the Ministry of Finance. As part of this effort, a steering committee (led by the Ministry of Finance and with the participation of the financial

[1] Computer Emergency Response Team.

regulatory entities) and a taskforce were created in order to implement the program and they have begun their activities to advance the program. In this context, the Banking Supervision Department is ensuring that the needs of the banking system in the cyber domain are included in the program and that the various tasks are advancing according to plan.

As part of its activity to improve the cyber resilience of the banking system, the Banking Supervision Department carried out a cyber exercise for the banking system in April 2022, in which for the first time the CEOs of the banking system were defined as the exercise's target audience. The Banking Supervision Department collated all of the insights gained in the exercise and presented them to the appropriate stakeholders in various forums. In December 2022, it distributed a letter to the banking system that described the main issues, the insights and the steps to be taken in the future.

As part of the efforts to increase the sharing of information and knowledge, which is intended to reduce risk and raise the level of protection in the banking system, the Interbank Cyber Security Forum held seven meetings during 2022, including a meeting with the Banking Supervision Department and the director of the National Cyber Directorate at the National Cyber Directorate's CERT center in Beer Sheva. In addition, there was ongoing activity to routinely monitor and evaluate cyber security at the banking corporations and in particular in domains with high cyber risk. In this context, an external scanning tool, which was made available to the Banking Supervision Department by the National Cyber Directorate, was periodically activated. This tool provides a picture of the level of cyber protection and information security in the supervised entities from an external perspective.

Evaluation of the banks' risk profile

During 2022, the Banking Supervision Department carried out extensive activity to periodically examine, evaluate and monitor the banking corporations and credit card companies. In this context, the Banking Supervision Department held meetings with their boards of directors and executives; it examined their strategic plans and their annual workplans, and analyzed their financial statements; etc.

Examinations and surveys in the banking system

The Banking Supervision Department is executing a long-term plan of examination missions[2] by means of teams of examiners with expertise in various types of risk. The goal is to identify and assess the variety of risks implicit in the various activities of the banking system and its compliance with the law and directives; to examine the performance of the management, control and corporate governance systems; and to bring about the identification of violations and their resolution.

[2] The Banking Supervision Department carries out examination missions on various scales and levels of quality, according to the objectives and circumstances. The method is chosen to achieve an optimal mix of examining the subject, the scope of coverage, and the depth of the inquiry.

Apart from the solution of problems, the findings are used to evaluate the functioning of the supervised entities and to identify needs with respect to regulation and enforcement.

The annual examination mission's workplan is formulated according to the principles of risk-oriented supervision and based on a process in which all of the information possessed by the Banking Supervision Department is weighted.[3]

Investigations carried out in 2022 focused on the following areas:

- Fairness in the marketing of consumer credit (see Box 7.7) and the pricing of credit lines.
- The quality of corporate governance in the formulation of policy, the supervision of the executive's work and the effectiveness of the gatekeepers—internal audit, risk management, and compliance.
- Terror financing prohibition risks: An examination of the bank's compliance with the relevant directives and an assessment of risk, as part of the national risk assessment of the banking system with respect to terror financing.
- The implementation of the new CECL[4] rules adopted by the banking system, including a review of the way in which account is taken of parameters in the banking corporations' credit risk management (see Box 1.3 in the Annual Survey of Israel's Banking System for 2021).
- The adequacy of processes to determine and document the actuarial assumptions used to calculate liabilities for employee rights.
- Improving disclosure in the banking corporations' financial statements.
- The assessment of credit risk in the construction and real estate industry, including the publishing of examples that arose in examinations, with respect to underwriting issues and problematic debt, and improving the reporting on credit to the industry.
- Aspects of syndication underwriting and environmental risk in the financing of infrastructure.
- A review of credit risk in the financing of activity abroad.
- The assessment of large groups of borrowers and an evaluation of borrowers according to indications of rising credit risk.
- Conduct risk in the trading room, with emphasis on fairness and transparency in trading and the adoption of the global code for activity in the foreign exchange market (FX Global Code) which was published in May 2017.

[3] The workplan can change or be revised as a result of significant developments or changing needs, according to the principles of dynamic supervision.

[4] Current Expected Credit Losses.

- The quality of counterparty credit risk for borrowers with large-scale and dynamic activity in the capital market.
- Examinations in the area of model risk, including the following: governance, policy and controls; development, assimilation and implementation; and efforts to validate the models. In this context, emphasis was placed on the management and monitoring of model risk, the adequacy of the models and their development process, the validation of the models and the use of models with high implicit risk. This was accomplished using tools from data science, economics, statistics, computer science and mathematics.

Stress tests of the banking system

As is standard practice worldwide, the Banking Supervision Department carries out a stress test of the banking system every year based on a uniform scenario. The stress test is a tool for the evaluation of the stability and resilience of the banks. Its goal is to identify the focal points of vulnerability within the various banks. The stress test in 2022 was characterized by a global shock, which spreads to Israel, as well as a slowdown in economic activity, and a drop in prices in the global and Israeli financial markets, alongside a rise in global interest rates as a result of the high inflation. Later on in the scenario, there is a slowdown in inflation and the central banks change direction by rapidly lowering interest rates in an effort to revive economic activity (see Box 5.1).

Business continuity

The increasing geopolitical threats, alongside the changes and developments in the business environment, require the banking system and the Banking Supervision Department to be well prepared for various emergency situations. The Banking Supervision Department's activity in 2022 focused on three areas: the promotion of preparedness for an emergency in the banking system; improving the Banking Supervision Department's readiness for an emergency; and the Banking Supervision Department's integration within the response to national events. This activity is reflected in, among other things, the supervisory regulation of the banking corporations' business continuity management; providing guidance and support; the execution of exercises; etc. (see Chapter 5.7).

Removal of the barrier to uploading core banking systems to the cloud

As part of the amendment of the cloud-computing directive, the banking corporations were permitted to made use of cloud computer services for core activities and systems. The banking corporations are required to set a policy for the use of cloud computing services. This includes, among other things, deciding on the characteristics of services defined as "a significant cloud computing service", subject to the aforementioned considerations and the management of the risk implicit in the use of cloud computing services in general (see Box 1.1 on the Proper Conduct of Banking Business Directive on Cloud Computing).

A review of the technological aspects of business continuity

Technology constitutes one of the components of every organization's business continuity plan. To ensure the continuity of critical processes, it is necessary, among other things, to ensure that the information systems that support them continue to be available during an event and that they will facilitate optimal customer service, while at the same time allowing workers to connect remotely, and provide them with support if necessary. Based on knowledge accumulated in the Banking Supervision Department from reports submitted to it, an exercise was carried out in 2022 that was based on a scenario of technological failure. The participating banking corporations were required to, among other things, carry out an analysis of the scenario's effect on their business activity and their customers and of the technological solution provided on the business side in order to deal with the failure event in both the short and long terms. The exercise's main challenge for the participating banking corporations was to analyze the effect of a localized failure event from a holistic end-to-end perspective of the business process, including the ability to identify all of the technological components that were affected. This called for a solution that would support business continuity on the service level and for a defined time period and not necessarily a solution that involved the automatic transition to a DR[5] site (see Chapter 5.7).

Monitoring of fraud prevention

An examination process was carried out in the system over the past year on the subject of internal auditing to prevent fraud. As part of this process, the banking corporations strengthened and enhanced their policies and the various control processes used to reduce the risk of fraud and embezzlement.

Granting a permit to Clal Insurance Company for the control of MAX

On September 1, 2022, a request was received from Clal Insurance Business Holdings Ltd. for a permit to hold the credit card company MAX IT Finance Ltd. (herein: MAX), which is controlled by Warburg Pincus, a private investment fund. After considering the request, a permit was granted.

Prudential Regulation

One of the principal means used to strengthen the stability of the banking system and to ensure its normal functioning is the issuing of regulatory directives. Following are the main areas in which the Banking Supervision Department was active in prudential regulation:

5 Disaster Recovery.

Salary payments to Palestinian workers

In June 2022, the Banking Supervision Department issued a letter on the subject of "Payment of salaries to Palestinian workers by way of bank transfers." In it, the banking system was asked to make the preparations needed in order to carry out salary payments by way of large-scale bank transfers and the development of an interface that will allow for the verification of data about the worker against the database of the Population and Immigration Authority. The project will provide an additional way to reduce risk. In December 2022, the Banking Supervision Department published a revision of the Proper Conduct of Banking Business Directive on Management of Anti-Money Laundering and Countering Financing of Terrorism Risks, which added the aforementioned requirement while defining the cases in which such a check must be made. During the second half of 2022 and the first quarter of 2023, the Banking Supervision Department continued its support of the preparations for implementing and dealing with supervisory issues that arose during the process (see Box 7.3).

Revision of the directive on the management of interest rate risk in the bank portfolio

The Banking Supervision Department is in the midst of a process to adopt the Basel directive on the management of interest rate risk in the banking portfolio. In June 2022, a draft directive on this issue was distributed within the banking system. The draft includes qualitative instructions for the management of this risk and also a description of the way in which the Supervisor of Banks is measuring it in the banking portfolio (standards for dealing with shocks), with the goal of generating results that are comparable to the estimated level of risk in the banking corporations and clearinghouses. A final directive is expected to be issued during 2023.

Operational deposits in the liquidity coverage ratio

The Banking Supervision Department revised the liquidity coverage ratio directives to allow for the recognition of operational deposits. These are the deposits of financial entities, and in some cases businesses, which are deposited with a banking corporation against the entity's activity at the banking corporation, but not for investment purposes or to obtain yield. As such, operational deposits are given a lower "withdrawal rate" in the liquidity coverage ratio and therefore their recognition improves the ratio. A banking corporation will be able to recognize operational deposits if it can demonstrate to the Banking Supervision Department that it meets the conditions of the directives. Furthermore, the rate of recognition is subject to quantitative limitations. The directive was revised following a comparison to the situation in other leading countries.

The activity of a banking corporation as a broker/dealer

In March 2023, a directive was distributed to the Advisory Committee on the subject of a broker/dealer that regulates the activity of the banking corporations in the area of financial intermediation, namely the receipt and conveyance of orders to carry out trades in securities for their customers, both in their activity as intermediaries and as part of their own trading activity. The goal of the directives is to protect investors and to maintain efficiency and fairness in the market, as well as reducing the risk of the banking corporations and in particular, the operational risk in the trading rooms.

The management of financial risk related to the climate and the environment

The Banking Supervision Department is continuing to promote the preparedness of the banking system and the Banking Supervision Department for financial risk originating in climate and environmental change. The resolution of this issue is spread out over a number of decades and includes the adoption of international standards for the effective management of financial risk related to climate and their inclusion within the draft of a new Proper Conduct of Banking Business Directive that was discussed last March in the Advisory Council for Banking Issues; the adoption of optimal practices for reporting to the public and disclosure to the Banking Supervision Department; creating supervisory and systemic abilities to carry out stress tests; membership in interministerial and interdepartmental forums in order to deal with data and information barriers; accumulation of knowledge through the monitoring of publications and professional literature, working papers and policy documents published by leading financial supervisory entities and international organizations; and membership in the workgroups and plenary body of the NGFS.[6]

Adoption of Basel directives on large exposures

The Basel directive on large exposures was translated before being distributed for preliminary discussion in the banking system. There was an internal discussion on various issues that are relevant to the Israeli banking system, and the decisions arising from the discussion were included in the directive. It was also decided to carry out a survey to understand the quantitative effect of the new directive on the level of concentration in the banking system.

Measurement and capital adequacy – operational risk

The Banking Supervision Department has initiated a process to adopt the revised Basel Committee directive regarding the calculation of capital requirements against operational risk, which constitutes part of the parameters that are referred to as Basel IV. It is expected that the final version of the directive will be published during 2023. It will include a future date for implementation, in order to facilitate the preparations for implementation.

[6] Network for Greening the Financial System—An international organization of more than one hundred central banks and supervisory entities.

Determining an increased risk weight for the financing of land acquisition

After the Banking Supervision Department detected an increase in the risk arising from the purchase of land for development or construction, it was decided to publish an amendment to Directive 203, which specified an increased risk weight of 150 percent when financing the purchase of undeveloped land at a rate that exceeds 80 percent of the asset's LTV.[7]

Sale of housing loans

The Banking Supervision Department has published a directive for the sale of housing loans and syndication to provide housing loans. The directive establishes the guidelines for carrying out transactions of this type based on the lessons learned from the Global Financial Crisis. They are meant to, among other things, protect the rights of borrowers in the loan portfolios that are sold, prevent a situation of negative selection that will lower the quality of the bank's credit portfolio and prevent the development of moral hazard for the purchaser.

Financial sanctions for violating the Prohibition on Money Laundering Law

The Prohibition on Money Laundering (The Banking Corporations' Requirements regarding Identification, Reporting, and Record-Keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order, 5761–2001, requires the storage of identifying documents for opening a bank account. The obligation to store identifying documents is an essential component of the regime for Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT). According to the international standards established by the FATF, the documenting and storage of identifying documents is meant not only to benefit the banks or the Banking Supervision Department, but also and primarily to meet the needs of enforcement agencies.

There were two technological problems that occurred in Bank Leumi's Pepper digital system, which led to a violation of the obligation to store documents for accounts opened online in 2021.

According to the law, it is possible to impose a financial sanction in the amount of NIS 2.26 million for a violation. The Committee for Sanctions against Banking Corporations[8] decided to reduce the size of the sanction relative to the maximum permitted by the law, given the fact that Leumi detected the violations on its own, reported them to the Banking Supervision Department, and acted to rectify the problem. Therefore, it was decided that the level of the sanction for the first violation will be about NIS 0.75 million and for the second violation NIS 1.13 million. Thus, the total of the financial sanction after the reduction was set at NIS 1.88 million.

[7] Loan to Value.

[8] The committee was created by the Prohibition on Money Laundering Law, 5760–2000. It has the authority, as part of the means of enforcement in money laundering, to impose financial sanctions on banking corporations (up to about NIS 2.26 million per violation) for violations of the law, as well as orders and regulations based on it.

Crypto activity

A Proper Conduct of Banking Business directive on the principles for the management of AML/CFT risk was amended in 2022 to include the activity of customers in virtual assets. In particular, the directive states that a banking corporation must carry out an appraisal of risk arising from the transfer of customers' funds where the source or the destination is crypto activity. Accordingly, a banking corporation is required to formulate a policy for its activity in this domain, and in any case, the directive establishes that it cannot refuse across-the-board to provide service for the receipt of funds by customers.

In February 2023, a revision was made to the Proper Conduct of Banking Business Directive on Risk Management, which requires banking corporations to report their activity in crypto assets to the Banking Supervision Department ahead of time. At the same time, a letter was sent out on the activity of banking corporations in crypto-financial assets (herein: crypto assets). The letter presents the main risks related to crypto activity and requires the banking corporation to view it as a product that should undergo the process for evaluating a new product and it defines the requirements that apply to the banking corporation in this domain (see Box 7.2).

Directives for reporting a new technology

The Banking Supervision Department attributes great importance to the appropriate management of information technology, in order to ensure the development of the banking corporation and the achievement of its objectives, while at the same time to prevent failures and achieve stability in the banking corporation's functioning, as well as the provision of digital services to its customers. To this end, a new prudential reporting directive was issued on technological indices. The main topics in the reporting directive are stability and availability; business continuity; cloud computing; resources, lines of defense and controls; strategic projects; and AI. This reporting will be used to assess technological risk among the banking corporations. The directive will go into effect in 2024 and will apply to the performance of information technology in the banking corporations in 2023.

3. THE MAIN ACTIVITIES TO INTEGRATE A CULTURE OF FAIRNESS TOWARD CUSTOMERS THAT IS INCLUSIVE AND IMPACTFUL

Consumer regulation

Mortgage reform to enhance transparency and comparability

Two revisions were made to the directive on procedures for the providing of housing loans and one to the directive on simplification of agreements. These revisions embodied the reform in mortgages, which introduces a series of measures meant to increase the customer's bargaining power, improve competition in the market, and streamline the process for obtaining a mortgage. The last objective has three components: transparency and comparability; simplicity and comprehensibility; and the efficiency of the process. These measures went into effect on August 31, 2022.

As part of these measures, the banks were required to provide the customer with an approval in principle in a standard format that includes, in addition to the mortgage basket being offered by the banks, three standard baskets for which their composition is determined by the Bank of Israel, where the term of the loan is chosen by the customer. The following will be included for each basket, among other things: the total expected interest; the total expected payments throughout the term of the mortgage; and the highest monthly payment expected according to the forecasts. In addition, the time for providing an approval in principle was shortened to a few days, and it was established that submitting a request and receiving approval will be possible online at all of the banks. Following the issuing of the directive, the implementation of the reform by the banks was monitored and improvements will be considered if necessary.

A new directive on the management of customer service and support

One of the main goals promoted by the Banking Supervision Department is the "assimilation of a culture of fairness towards the customer that is inclusive and impactful." The quality of service provided to customers constitutes an important component in fair behavior towards customers. In order to improve the quality of services, the Banking Supervision Department published a Proper Conduct of Banking Business Directive on Managing the Customer Service and Support System. The directive formalizes the principles for providing service and support to customers and defines the obligations in the area of corporate governance and duties to establish a service covenant and to publicize information about customer service and support, with the goal of promoting an organizational culture that emphasizes the quality and availability of service and support for customers, which will in turn increase transparency for customers. The directive was issued on March 29, 2023 and for the most part will go into effect within a year from that date.

Publishing a Supervisory Order for basic checking account fees in order to freeze prices

The Banking Supervision Department published a supervisory order for basic current account fees for the public's benefit and with the goal of freezing the current levels. The services over which supervision will be extended are the following: a teller-executed transaction; a customer-executed transaction; the expanded track; and the expanded plus track (which went into effect on September 1, 2022). The basic track is already under supervision and its maximum price was set at NIS 10.

A new directive on advanced means of payment

In view of the expansion in the number of payment transactions carried out by payment apps, a Proper Conduct of Banking Business directive on advanced payment services was issued on June 19, 2022. The directive expands the information presented to customers with current accounts and payment cards with regard to the customer's activity in payment apps. The directive complements the Payment Service Law, 5779–2019 and formalizes the information that will be presented to the customer.

Directive on the "Opening of a checking account without a credit facility and account management"

The directive was expanded to include the management of a current account with a negative balance that does not exceed the approved credit limit, in addition to the management of a current account with a positive balance. The goal is to ensure that these customers are also provided access to basic payment services and to information through the digital channels. In addition and given the importance of providing banking services to all customers, it was decided to revise and clarify the existing instructions in the directive by specifying that across-the-board rules are not be applied in order to block a customer's activity only because he belongs to a particular population. Furthermore, the basic payment services provided by the directive were expanded. A revision of the directive was issued on March 29, 2023.

The impact of the Russia-Ukraine war

The impact of the war, as it affects the banking corporations in Israel, constitutes one of the many challenges in risk management, in view of the exposure to risk of violation or circumvention of the international sanctions imposed on Russia. Therefore, the Banking Supervision Department has distributed various letters, such as the Supervisor of Banks' letter on the "Risks implicit in contracting with parties appearing on the international sanctions lists and on the national sanctions lists of foreign countries", which was distributed in June 2022. According to the letter, the banking system is required to formulate a policy and procedures with regard to the use of international and national sanctions lists and contracting or doing business with listed entities. This was motivated by the potential risk of the banking system being exploited in order to circumvent the sanctions regime.

In addition, the Banking Supervision Department has operated, and is continuing to operate, in a variety of ways with the goal of helping new immigrants who are encountering difficulties in the banking system. The main message is that the banking system must work with sensitivity and should make their services available to new immigrants. These messages are also reflected in two supervisory letters that were published by the Banking Supervision Department: "Opening of accounts for new immigrants and the receipt of funds from Russia by way of the banking system in Israel", from August 2022, and "Providing service to customers of the Israeli banking system against the background of the war between Russia and Ukraine", from February 2023, which includes clarifications that are intended to assist new immigrants who came to Israel as a result of the war (see Box 7.4).

Closure and transfer of branches

The Supervisor of Banks distributed a letter to the banking system that requested that they meticulously fulfill the requirements in the directive on "Closure of bank branches and reduction of teller services", with emphasis on examining the geographic distribution of branches and the circumstances of each case, based on the approach of the "customer at the center" and an understanding that branches and face-to-face services have not become redundant.

Consumer fairness in a changing financial environment

In light of the changes in the interest rate and inflation environment, the Supervisor of Banks distributed a letter to the banking corporations in which he emphasized his expectation that the interests of customers be protected, in view of the aforementioned developments, and to ensure that the interests of customers should be the focus. In addition, the Supervisor of Banks updated the Banking Supervision Department's intention to publish the interest rates granted by the banks in actuality—which was indeed published, as described below.

Clarifying letters on various issues related to bank fees

The Supervisor of Banks distributed a number of letters related to bank fees, which were intended to clarify various issues for the benefit of customers. Among the issues dealt with in the letters: disclosure of the cost of service in the case of third-party expenses; third-party expenses that accompany the provision of credit; a fee for the submitting of a request for a housing loan following the amendment which established a maximum fee that a banking corporation can collect for processing a request for a housing loan.

Increasing the transparency of consumer enforcement

The Banking Supervision Department advised the banking corporations of its intention to publish ongoing updates on the Bank of Israel website concerning additional steps taken against supervised bodies, including a requirement to reimburse a group of customers, as a result of the handling of systemic cases by the Public Enquiries Unit.

Involving banking corporations and credit card companies in the process of evaluating fairness in the banking system

The Banking Supervision Department has invited the banking corporations and the credit card companies to carry out an internal brainstorming process on the evaluation of fairness and to submit proposals to improve its methodology.

Restricting a closed checking account – delivering notifications to the customer

A clarification was issued that according to the law there is an obligation to send notifications of a restriction on an account, even in cases in which the account is closed.

Periodic publications meant to increase fairness toward customers of the banking system

Interest rates: Publishing comparative information of the interest rates on deposits and credit

As part of the examination and analysis of the transmission mechanism, the importance of transparency and the shift of power to the customer, the Banking Supervision Department published the interest rates actually paid on shekel deposits (fixed rate and variable rate interest, and interest actually collected for the providing of variable-interest-rate credit), with the goal of enabling customers to make informed decisions on the basis of a simpler, more accessible and more convenient comparison of the terms offered by the various banking corporations. The information on the website is updated every month, and in February 2023, the information provided was expanded, with the goal of offering the public complete and detailed information so that it can more easily compare the interest rates of the various deposit and credit products. During 2023, the Banking Supervision Department will also publish data on the website with regard to the rates of interest actually collected by the credit card companies.

Bank fees: Periodic reporting of the prices of common banking services used by households

In September 2022, the Banking Supervision Department published the periodic report on the prices of common banking services used by households. The report is based on the reporting of actual revenues collected by the banking system and credit card companies in 2021.

Telephone response: Periodic report to the Knesset Economic Affairs Committee on the compliance of the banking corporations with directives for the waiting time to receive a professional human response

In July 2022, the Banking Supervision Department published the periodic report submitted to the Knesset Economic Affairs Committee on the compliance of the banking corporations with the directives regarding waiting time for a professional human response. The report includes comparative data on the waiting times for each of the banking corporations and general data on the period being reported.

Handling of public enquiries by the Banking Supervision Department during 2022[9]

The Banking Supervision Department's Consumer Enquiries and Inspections Unit handles the enquiries received by the Banking Supervision Department on the activity of the banks and credit card companies, from the perspectives of both the customer that submitted the complaint and the entire system. The goal is to identify and resolve problems in the activity of the banking corporations or the banking system as a whole, as experienced by the customer.

The Unit received about 10,000 requests for information and complaints from the public in 2022. In addition, the Unit's call center provided a response to more than 15,000 telephone enquiries.

Following are the data on requests for information and complaints received in writing:

a. **Direct handling** – The Unit dealt with about 5,400 enquiries, of which about 1,800 were complaints and about 3,600 were requests for information.

b. **Handling by means of exhaustion of proceedings** – About 4,600 complaints received by the Banking Supervision Department were submitted to the ombudsmen of the banking corporations and credit card companies, according to the guidelines set down in Proper Conduct of Banking Business Directive 308A – Handling of Public Complaints.

The handling of public complaints includes an examination according to the law and the determination of remedies to be provided to customers in the appropriate cases. In this context, about NIS 1.3 million was refunded to customers in 2022 as a result of the direct handling of individual enquiries.

Consumer monitoring and the resolution of significant systemic problems

- The handling of enquiries from the public provides opportunities to correct problems and flaws, to deal with existing problems on a systemic basis and to draw conclusions that lead to the improvement of service provided to the banking corporations' customers. In addition, the Banking Supervision Department initiates proactive audits in order to increase consumer-oriented compliance. In cases where significant failures are identified based on enquiries from the public and on the findings of enforcement audits, the Banking Supervision Department will require that the problem be resolved by means of, among other things, reimbursements of the affected customers. As part of the systemic resolution of problems, a total of about NIS 4.5 million was reimbursed to customers in 2022 and 2023 (up to the time of writing). This included a variety of reimbursement types: the collection of bank fees at a higher rate than what appears in the bank's price list; nonprovision of discounts to customers, in violation of the bank's published terms; and the collection of payment card fees before the card was activated, in violation of the price list.

[9] The Banking Supervision Department's Survey of Public Enquiries and Measures to Protect the Consumer, which is published annually on the Bank of Israel website, includes the Banking Supervision Department's activity to check the complaints and how they were resolved, as well as activities in the area of enforcement and the resolution of systemic problems in the banking system.

- The proactive enforcement examinations are carried out from time to time in areas on which the Banking Supervision Department is focusing. In 2022, the focus was on the cancellation of pledges, which revealed pledges on customers' assets that were not cancelled after the loan for which the pledge served as collateral was paid in full, as required by law. As a result, the Banking Supervision Department required the resolution of the problem and instructed the banks to carry out a more comprehensive examination in order to ensure that pledges for loans that had already been redeemed had been cancelled. As a result of this requirement, more than 30,000 pledges were cancelled in the banking system.

- In cases where significant problems are identified, the Banking Supervision Department uses its authority to impose a consumer-oriented financial sanction on the banking corporation. The Banking Supervision Department imposed a financial sanction of NIS 650,000 on Cal in 2022. This followed an examination carried out by the Banking Supervision Department that revealed that the company had, in certain circumstances, honored debits received on a credit card that had been cancelled. A different examination regarding the collection of debts revealed that Discount, Poalim and Mizrahi-Tefahot had not complied with a Proper Conduct of Banking Business Directive concerning the collection of debts from customers. As a result, in February 2023 it imposed financial sanctions of NIS 1,200,000, NIS 850,000 and NIS 700,000, respectively. The financial sanctions were imposed due to nonreporting to the Execution Office of payments made toward a debt. An additional financial sanction was imposed on Discount for nonreporting to the Execution Office, within a reasonable period of time, of a debt restructuring arrangement between the bank and the customer.

Restricted accounts

- As of December 31, 2022, there were 525,652 restricted accounts. There were 270,822 restricted customers, of which 251,260 had a special restriction imposed on them by one of the collection entities (the Collection Authority; the Official Receiver; the Center for Collection and Fines and the rabbinic courts) and 19,562 had a "bank" restriction imposed on them (as a result of writing a check without sufficient cover).

- Following the sharp drop in the number of customers on whom a "bank" restriction was imposed (as a result of writing a check without cover) during the period following the onset of the COVID-29 pandemic and the exemptions that were put in place as a result, an upward trend in their number began to appear—from 15,937 at the end of 2021 to 19,562.

- During the course of 2022, the Banking Supervision Department dealt with 3,449 enquiries in writing regarding restricted accounts and in parallel 47,116 customers made use of the personal area that provides unique personal information and can be used to produce confirmations for restricted customers.

Financial Access Covenant

The Financial Access Covenant was launched in January 2016 with the goal of mitigating the consequences of economic abuse against battered women who are living in shelters and halfway houses. This involved the meeting of these women's needs through appropriate financial solutions, in order to help them deal with the economic abuse they have experienced and to turn over a new leaf. The annual covenant meeting took place in March 2022. As part of the annual revision of the covenant, emphasis was placed on two new components: The first is the completion of the pilot program and the expansion of the covenant to 169 domestic violence centers throughout the country. Thus, the financial institutions that are part of the covenant are prepared for its expansion to all of the centers operating in Israel. The second deals with a situation in which the debts owed to the victim of abuse include debts to other creditors, which hinders the assistance provided to the victim by the financial institution.

In 2023, the covenant was expanded to include prostitution survivors, based on the understanding that their economic situation has a major impact on the degree of their rehabilitation and that financial difficulties are a major barrier on the way to recovery and rehabilitation.

Encouraging Social Impact Banking

The area of Impact Banking, which includes the banking corporation's social responsibility, has gained momentum in recent years in the global banking community. The idea underlying Impact Banking is that a banking corporation should act with the goal of benefiting society and the environment, in order to strengthen the public's trust in the banking system. This should involve the exploitation of the banking system's potential to generate impact, by means of adding social considerations to its various business considerations.

The Banking Supervision Department is promoting this goal by creating a comparative index that will be made available to the public. This index will motivate the banking system toward change, will create a basic standard for the behavior of all the banks, and will help strengthen the public's trust in the banking system. A draft questionnaire has been distributed in the banking system in order to obtain its initial feedback.

Increasing financial awareness in Arab society

In partnership with the Center for Local Government, the Association of Banks and the banking system, the Banking Supervision Department led a campaign in June 2022 to increase financial awareness in Arab society. This included dozens of Arab towns throughout Israel and thousands of participants. The activity included lectures in Arabic on "How to manage my money correctly" and personal guidance in the bank branches. In view of the importance of this subject and with the goal of enabling additional Arab citizens to acquire the tools for responsible financial management, the campaign was repeated in December 2022.

Surveys of satisfaction among households, self-employed businesses and small and micro businesses

In December 2022, the Banking Supervision Department published the findings of a 2022 survey of customer satisfaction with service provided by the banking system. Following are the main findings of the survey of households for 2022, as compared to those of the 2021 survey:

- Satisfaction with the use of the banks' websites remains high.
- Satisfaction with the use of the banks' apps remains high.
- There has been a drop in satisfaction with service provided by the call centers.
- There has been a drop in satisfaction with service provided at the branches.
- There was no change in the fairness of the banks as perceived by customers.

Similar findings emerged from the survey of self-employed businesses and small and micro businesses. Note that availability and individual attention were described as two important needs in relations with the bank. However, satisfaction with the banks' availability and their familiarity with the businesses' activity was low.

4. THE MAIN ACTIVITIES TO CREATE A MORE COMPETITIVE AND ADVANCED FINANCIAL SYSTEM FOR THE BENEFIT OF CUSTOMERS

The promotion of open banking – Open Banking API

The Banking Supervision Department continued to take a leading role in the promotion of open banking in Israel, which is essentially the providing of access for a third party to a customer's account, with the customer's consent, and with the goal of obtaining information or carrying out some activity. The Banking Supervision Department's vision is to expand the world of open banking such that the entire financial system will eventually become part of Open Finance. Open banking activity constitutes the first milestone in modifying products and processes in the world of banking and finance, at the center of which lies the asset of information possessed by the customer, and it works to leverage that information using technology for the benefit of the customer. The Financial Information Service Law, 5772–2021, which was legislated in November 2021 and went into effect in June 2022, presented a timetable by which baskets of information in Open Banking will be gradually introduced until the end of 2023. So far, the banking system has made available information on checking account activity, credit card activity, deposits and credit provided to individuals and small businesses. In addition, the Banking Supervision Department has worked to create a standard for the externalization of information on activity in securities. Looking to the future, it is reasonable to assume that Open Banking will expand into Open Finance and perhaps even Open Data, which will have a systemic impact and will of course have an effect on the various market players (see Box 7.1).

The reform in switching banks

In September 2021, a reform initiated by the Bank of Israel and the Ministry of Finance went into effect that requires the banking system to allow customers to switch banks in a convenient, speedy, secure and costless process. The reform had the following goals: to increase competition between the banks; to allow new players to offer financial services; to make it easier to switch banks; and to enable customers to improve their terms, whether at their existing bank or at a new bank, by increasing their negotiating power.

A year after the introduction of the reform, in December 2022, the Banking Supervision Department published additional information about the process, which included data received from the online system; monitoring of the banks by the Banking Supervision Department; and the findings of a survey of customer satisfaction carried out a year after the initiation of the reform. In November 2022, there was another phase in the information campaign on the Internet in order to increase the public's awareness of the online system and the possibility of switching banks conveniently and online.

Creation of a digital guarantee system

The project to create a digital guarantee system is intended to facilitate a fully digital process for issuing guarantees and submitting them to government organizations. It will primarily be government ministries that will work with the system in the first stage by means of the Merkava system. Designated systems that will gradually join the system are located in the Population and Immigration Authority, the Israel Land Administration, the Customs Authority and the police. The Israeli banking system also gradually joined the digital guarantee system during 2021 and 2022. On September 1st, 2022, the transition was made to the digital guarantee system (with some exceptions) and, according to a government decision, the government ministries (with some exceptions) will only accept digital guarantees starting from January 2023.

Payment apps

On January 15, 2023, an arrangement went into effect that is based on the Proper Conduct of Banking Business Directive on Identification and Verification of Customers during the Providing of Payment Services by the Banking Corporations. The arrangement provides exemptions from identification and verification requirements that are incumbent on the banking corporations when providing certain payment services.

The activity of regulated financial service providers vis-à-vis the banking system

During 2021–22, the Banking Supervision Department carried out a comprehensive examination of the banks' policy regarding regulated financial service providers. The Banking Supervision Department is currently working on the introduction of a biannual reporting directive regarding the banks' reporting on accounts of regulated financial service providers.

Regulating payment services and payment initiation

At the beginning of 2023, a legislative proposal was published for the regulation of payment services and initiation of payments. The proposal was made by the Ministry of Finance, the Ministry of Justice and various regulatory financial entities (the Bank of Israel, the Israel Securities Authority and the Capital Market Authority), as well as the Competition Authority. The goal of the legislation is to regulate the supervision of payment service providers and to determine which entity is to supervise them, their obligations, the process for obtaining a license, the activities permitted to them, etc. The law establishes that payment services providers that are neither banks nor auxiliary corporations will be supervised by the Israel Securities Authority. Nonetheless, at this stage, systemically important payment service providers, including the credit card companies, will be supervised by the Bank of Israel.

In addition, the proposed legislation formalizes the obligation of the payment account managers to allow access to customers' accounts for payment initiators, in order to write payment orders or permissions to debit an account or cancel permissions to debit an account. Two obligations were established for the initiation of payments: The first is basic initiation—in which the customer approves the payment instruction with the payment account manager; while the second is advanced initiation—in which the customer gives permission to the payment initiator to send payment instructions for execution and subsequently, and for each payment, the customer approves the payment instruction with the advanced initiator. As the legislation progresses, the Banking Supervision Department will continue to issue directives and regulations that are suited to additional types of payment initiation.

Guidance and support for the creation of new banks

Completion of the process to create One Zero the Digital Bank Ltd.

On January 9, 2022, the restrictions were removed from the license of One Zero the Digital Bank Ltd. (herein: the bank), after it achieved the milestones for its establishment. Thus, the license it was granted on December 13, 2019 became a license without any time limits or restrictions. This is the first bank to obtain a license in more than 41 years. The Banking Supervision Department is monitoring the activity of the new bank as part of the ongoing monitoring process for a new small bank. Specifically, it is monitoring the risks to which the bank is exposed and the implementation of its workplan.

Issuing a conditional bank license to the esh Israel Bank (in formation) Ltd.

On December 25, 2022, the esh Israel Bank (in formation) was granted a banking license. The license is conditional on meeting the milestones specified in the license and has not yet been operationalized. The creation of the bank is being guided by a steering committee headed by the Supervisor of Banks and with the participation of the various divisions in the Bank of Israel, which are providing close support for the creation of the bank and are verifying that it meets its milestones.

Control permits and licenses for new clearing houses

The Banking Supervision Department is examining additional requests for clearing licenses for new clearing houses. The examinations are focusing on the personal and business integrity of the applicants for the control permit, their financial resilience and their ability to absorb the expenses required to establish and operate a new clearing house. The Banking Supervision Department is also looking at their business plan and its feasibility.

The separation of Cal and Discount

In accordance with the Banking (Licensing) (bank with a broad range of activity) Regulations, 5783–2023, Discount Bank will be required to sell its holdings in Cal Ltd. within a period of three years (or 4 years under certain conditions). The Banking Supervision Department is guiding the separation process.

5. THE MAIN ACTIVITIES TO ADJUST THE BANKING SUPERVISION DEPARTMENT'S OPERATING MODEL TO A CHANGING ENVIRONMENT

The Banking Supervision Department's vision is "to provide professional and proactive supervision that will benefit the public and the economy." As part of the activities to achieve this vision, the Banking Supervision Department has worked to strengthen its role on a number of fronts, so as to keep up to date with recent trends, existing tools, new information and the appropriate areas of emphasis. Following are a number of examples:

SupTech – Supervisory technology

During the second half of 2021, the Banking Supervision Department initiated a project to formulate a vision to maximize the value obtained from information and the possible steps to create business value. Among the measures considered, two were chosen during 2022 as having significant value to the Banking Supervision Department and also high feasibility: warnings and publicizing of information. During the second half of 2022, workshops were held with workers and managers in order to select scenarios for the desired warnings. Two scenarios were selected: proximity to a limit and identification of outliers (see Box 7.5).

Implementation of the Regulatory Principles Law

The Regulatory Principles Law, 5772–2021 (herein: the law), which went into effect on January 1, 2023, applies to the Bank of Israel as a public corporation and relates to its authority in the regulation of banks, clearing houses and sharing of credit data. The goal of the law is to advance the optimal regulation by government entities and public corporations which is meant to achieve a clear goal that is grounded in the regulator's authority and that will constitute effective regulation that does not impose any excess regulatory burden. In December 2022, the Banking Supervision Department published instructions regarding the execution of the report by issuing regulations according to the Regulatory Principles Law, and it has been implementing the instructions of the law in 2023.

An examination of the Banking Supervision Department's operating model

In light of the changes that have occurred in recent years in the financial domain (in Israel and worldwide) in the macroeconomic environment, in regulation, and in the technological, prudential and consumer/social domains, there is a need to reexamine the Banking Supervision Department's work practices, its work processes, its supervisory capabilities, and the appropriateness of its resources and their suitability to a changing environment, based on a forward-looking perspective (herein: the Banking Supervision Department's operating model), with the goal of being a leading supervisory authority. During 2022, the Banking Supervision Department examined its operating model and worked toward the improvement of its internal work processes.

The Supervisor of Banks delegation to Singapore and Australia

In November 2022, a delegation of the Banking Supervision Department's managers, headed by the Supervisor of Banks, traveled to Singapore and Australia. The delegation met with representatives of central banks, supervisory authorities, commercial banks, international advisory bodies, etc. The delegation dealt with a wide range of subjects: supervisory approaches; risk, climate and the environment; innovation and technology; business behavior; licensing and new digital banks; etc. Insights regarding the future work of the Banking Supervision Department, based on the highest international standards, were integrated within the department's workplans.

Formalizing the connection with US supervisory authorities and improving the mechanism for information exchange

The Banking Supervision Department is continuing to maintain and manage its working relationship with financial supervisory authorities abroad, as part of its Home-Host relationships, as required by formal agreements signed with those authorities and in accordance with the recommendations of the Basel Committee. In this context, the Banking Supervision Department worked to strengthen the formal mechanism for exchange of information between the Banking Supervision Department and the three financial supervisors in the US that are responsible for the branches of Israeli banks located there: the NYSDFS, the Fed and the FDIC.

Box 7.1
Open Banking

- The regulation of open banking has developed and coalesced in recent years, worldwide as well as in Israel. The activity in open banking began in April 2021 with the issuing of the Banking Supervision Department's directive to the banking system; starting in June 2022, it was based on the newly passed Financial Information Services Law.
- Toward the end of 2022, there was a jump in the usability of the system. Our assessment is that to the extent that the system continues to develop and stabilize, and as the public becomes aware of it and relies on it, use of the system will increase significantly.
- The complexity of the system from the technological and regulatory viewpoints creates challenges for participants, and they need to collaborate in order to solve the problems that are liable to arise. It is expected that organized and consistent efforts will be made by both data sources and financial information service providers.
- Open banking has led to further initiatives to expand the sharing of information in other contexts, including nonfinancial ones. Worldwide, there are initiatives to share information in the domains of insurance, infrastructure, health and even initiatives to share all information.

Introduction – The global development of open banking

The comprehensive regulation of open banking worldwide has developed to a great extent in recent years, including the EU's Payment Services Directive 2 (PSD2)[1] and the Consumer Data Rights (CDR)[2] regulation in Australia. These regulations strengthen customers' control over their financial information and the way in which transactions are carried out in their bank account, to the extent that they require the banks to provide an authorized third party with access to the customer's account (subject to the customer's consent), and to share the banking information and to write payment instructions for the customers.[3] Based on access

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
[2] https://www.cdr.gov.au
[3] There are three main entities in open banking systems: customers—an individual customer or a corporation who wishes to consume open banking services; third-party providers who wear two hats—as consumers of information when they request information on the customer from a data source (in Israel this is known as a financial information service provider; a service provider) and as a payment initiator who writes a payment order for the customer that subsequently requires the approval of the financial entity; and financial entities that also wear two hats—as data sources that are required to provide information to the service providers and as the managers of a payment account who are required to receive the payment instruction from the payment initiator.

to these accounts, the third party providers will be able to offer new products and services to customers that are personalized and improve the customer experience. The establishment of an open banking ecosystem[4] will allow for and encourage the entry of new players in related financial service domains: payments, information, intermediation and more. This essentially will enable the customers to obtain a better picture of their financial situation, to consume more innovative services in these and other domains, to obtain financial services from a variety of providers (disaggregation of financial services) and to obtain value proposals that are more competitive in general as well as those that are personalized for the customer.

These regulatory directives create clear rules for the licensing requirements that apply to third-party providers, responsibility agreements, information security rules, etc. while at the same time leaving room for the development of an ecosystem at a pace that is in line with the development of the technology and new services for the customer. Clearly, there is a different perspective regarding the requirement to make information available to third parties, including the creation of an appropriate regulatory infrastructure for the development of an open banking ecosystem. In Europe, Australia, Brazil and other countries, the regulatory infrastructure has been critical for this development, i.e., it has been regulatory-driven, while in the US the development has been market-driven.

At the same time, the understanding has emerged, whether in the market or among regulators, that the existence of an open banking standard that will determine the business and technological rules of the game for the participants is another important component in the development of the open banking ecosystem and at a later stage a system of open data as well. In light of this understanding, there are various initiatives worldwide to formulate a uniform standard, whether at the initiative of the market or the regulator (Britain, the Berlin group, STAT, Australia, etc.). The open banking activity and the consent of the customer are described below in Figure 7.1 and 7.2.

In this box, we will first describe the development of open banking in Israel, the manner in which it is being implemented in Israel, the challenges in its implementation, the development of open banking in the future and initiatives for the sharing of information worldwide.

[4] A system of individuals with reciprocal relations between them. In the business context, this is the system of relations between the parties involved in a product or technology, such as producers, providers and customers (from the Avnion Dictionary).

Figure 7.1 The Process of the Customer's Consent

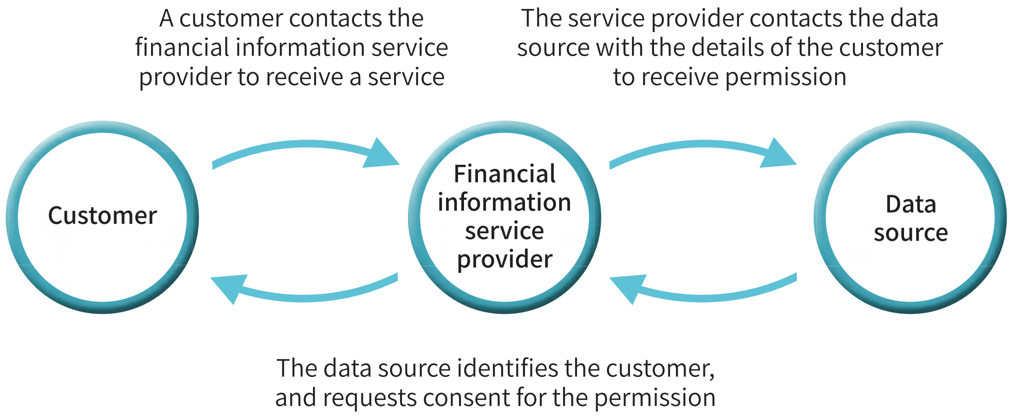
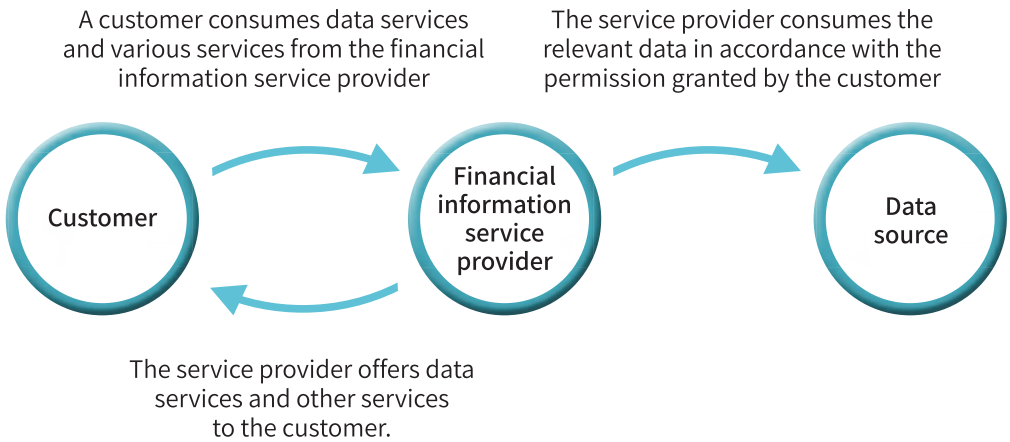


Figure 7.2 Open Banking Activity



The development of open banking in Israel

Processes to achieve the sharing of information began in the context of the Increasing Competition and Reducing Concentration in the Israeli Banking System (Legislative Amendments) Law, 5777–2017, which established that the provider of a cost comparison service will be given access to the customer's account by way of a unique password. Nonetheless, there were no directives issued in this domain and therefore, based on the law, the section did not go into effect. At the same time, and despite the lack of orderly legislation or appropriate regulations, the Bank of Israel continued to promote the open banking environment, due to the importance attributed by it to promoting innovation and competition in financial services and the huge potential of this activity. The Bank of Israel adopted the goal of promoting competition in the banking system and improving the customer's position by means of data sharing in the banking system, at first as an enabling regulator and later on as an obligating regulator. The Bank of Israel, as a path-breaking regulator, not only made the implementation of open banking mandatory even before there was legislation in this domain, but it also worked toward the adoption of an international standard, based on the understanding that a shared international language would support the entry of additional participants into the ecosystem. The Bank of Israel has invested major efforts in promoting an efficient open banking ecosystem and views the advancement of open banking as one of the Bank's flagship projects.

Accordingly, the Banking Supervision Department formulated a Proper Conduct of Banking Business directive that defines, among other things, an API-based uniform technological standard for the entire open banking ecosystem, which will allow new players to enter. Following a thorough review, which included consultation with experts in Israel and abroad and with various players in Europe and Israel (banks and fintech companies), the Bank of Israel decided to adopt the Berlin Group's NextGenPSD2[5] standard, with the appropriate modifications to the Israeli economy.

In February 2020, it published Proper Conduct of Banking Business Directive no. 368 (hereinafter, **"the Directive"**), which defines the manner in which the open banking standard is to be implemented in Israel. The directive was written following discussion among all the relevant players in the ecosystem,[6] based on the understanding that open banking will affect numerous entities in the economy, not only the banking system. The directive in its initial version applied to the banks and the credit card companies, because they are supervised entities. The goal was to develop an infrastructure for open banking in which the banking system serves as the data sources. After the approval of the legislation, additional entities, given the appropriate regulation, will be able to join the system relatively quickly and with shortened timetables. Accordingly, an open banking system went live for the first time in Israel in April 2021. From that point onward, the banks in Israel have made it possible for customers to grant access to the information in their current accounts in a digital and secure manner to third parties from within the banking system. In addition, the directive established

[5] The Berlin Group is a pan-European initiative whose main goal is to define a technological standard for the use of various participants in the PSD2 regulation. The group consists of members located throughout Europe, and since 2019, the Bank of Israel has been a member.

[6] The banking system, fintech companies, the Ministry of Justice, the Ministry of Finance, the Capital Market Authority, the Israel Securities Authority, the Competition Authority, the National Cyber Directorate and Digital Israel.

conditions and instructions for payment initiation service[7] in the open banking world. At this stage, the obligation applied only to a single payment initiation (not future dated), with the goal of creating a strong base for the initiation of payments.

In November 2022, the **Financial Information Services Law**, 5782–2021 was published, and went into effect in June 2022. It formalizes the entire range of activities included in the provision of financial information services, both from the side of the financial information service provider[8] (third-party providers of the service to the customer) and the side of the data sources[9] (the financial entities that are required to provide access to the financial data of their customers). Accordingly, the Proper Conduct of Banking Business Directive has been revised to include arrangements appearing in the aforementioned law and the timetables it specifies.

Following is the timetable established in the directive and in the Law for the Implementation of Information Baskets by the Banks and Credit Card Companies:

Date of implementation	Data baskets and initiation services	Source
April 2021	Current account data.	Directive 368
March 2022	Payment card data; single payment initiation.	Directive 368
June 2022	Credit (loans) data; Savings data.	According to the law
January 2023	Expansion of the data on corporations with a turnover of up to NIS 5 million that have a single signatory.	According to the law
June 2023	Data on securities.	According to the law
December 2023	Expansion of data on all corporations.	According to the law

7 Initiated payment service activity involves the writing of the payment instruction, which will be approved by the payer and executed accordingly by the manager of the payer's account, who is not the one who writes the payment instruction.

8 According to the Financial Information Service Provider Law, this is an entity with a license to provide financial information services or the owner of a permit to provide financial information services. The law allows numerous entities to become financial information service providers, including fintech companies, banks, credit card companies, credit bureaus, institutional entities, etc.

9 The law defines the following entities as data sources: a bank, an auxiliary corporation (as defined in the Banking (Licensing) Law, an institutional entity, the owner of a license to provide deposit and credit services; the owner of a credit provider's license; the owner of a license to operate a credit intermediation system; other entities that will be decided on according to Section 68(c) of the law. As of now, only banks and credit card companies are serving as data sources.

Despite the short timetable, the banking system complied with the requirements to expand the information that is accessible within the open banking environment. Nonetheless, it is worth mentioning that the timetable defined in the law constitutes a challenge with regard to the implementation of open banking in the case of data on securities and the expansion of information to include large corporations. The adoption of an international standard requires modifications to fit the Israeli financial market, including its unique products and certainly in light of the fact that no standard for securities existed and that the standard was issued by the Berlin Group only in November 2022.[10]

The implementation of open banking

The law establishes the regulatory framework, including the identity of the entities defined as data sources and the identity of the four regulatory entities (the Banking Supervision Department, the Capital Market Authority, the Israel Securities Authority, and the Credit Data Sharing System) who are empowered to grant a permit or license[11] to operate as a financial information service provider in the ecosystem. Starting from the fourth quarter of 2022, the number of service providers who have received approval from the Banking Supervision Department or a license from the Israel Securities Authority has increased significantly. As of March 2023, about 22 entities[12] had received approval or a license to operate in the ecosystem as a "service provider".

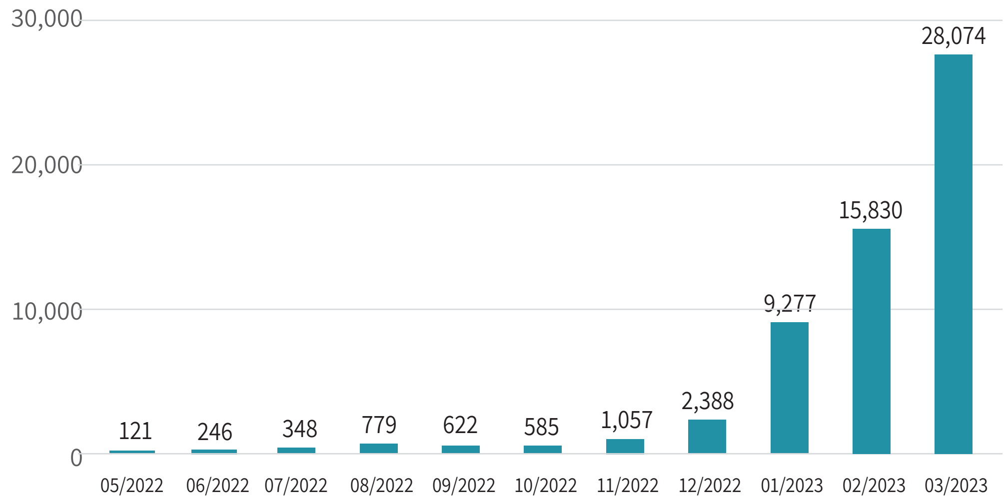
As can be seen in the two graphs below, there has been a significant increase in activity in the ecosystem, which is due to the increase in the number of service providers, the stabilization of the system and the growing awareness of open banking among customers. In November and December 2022, there has been a significant increase in API requests, where the number of requests received was about 1 million and about 2.4 million, respectively. This in comparison to about 240,000 in June 2022 when the law went into effect (at the five largest banks). Starting in January 2023, there was another large jump in the number of requests in the system (the entire banking system), reaching about 28 million in March 2023. This was due to the combination of requests by service providers submitted to the credit card companies at the same time as the stabilization of the systems among data sources and among service providers.

10 In light of the short timetable for the implementation of a securities information basket and based on the Governor of Israel's request, the Minister of Finance published a draft financial information service directive to solicit the comments of the public regarding the deferral of the application of the law in the domain of securities and accounts of large corporations. The draft proposes a delay in the application of the Securities Information Law until October 15, 2023 and a delay in the application of the requirement to provide access to data on the accounts of large corporations until April 14, 2024.

11 Financial entities that have different licenses (such as a bank, credit bureau or financial entity with a permit to provide credit) are required to obtain approval from the authority that supervises them. Nonfinancial entities (such as fintech companies) are required to obtain a license from the Israel Securities Authority.

12 The group consists of nine entities in the banking system that have received approval from the Banking Supervision Department, ten entities that received a license from the Israel Securities Authority, and another three that are supervised and received approval from the Capital Market Authority. Following is a link to the Bank of Israel website on this topic: https://www.boi.org.il/roles/supervisionregulation/16992. [Hebrew]

Figure 7.3 Number of API Enquiries Received,[1] May 2022–March 2023 (thousand)



1 2022 data include enquiries to the five large banks only. From January 2023, the data relate to enquiries to the entire banking system.

SOURCE: Based on reports to the Banking Supervision Department.

It can also be seen that the number of "consents"[13] in the five largest banks is increasing accordingly. Prior to the law going into effect, the number of standing consents at the end of the first quarter of 2022 was about 487 while at the end of the second quarter of 2022 it was about 1,286. In contrast, there was a large increase after the law went into effect, such that the number of standing consents at the end of the fourth quarter of 2022 was about 11,988 while at the end of the first quarter of 2023 it was about 34,239.

Challenges in the implementation of open banking

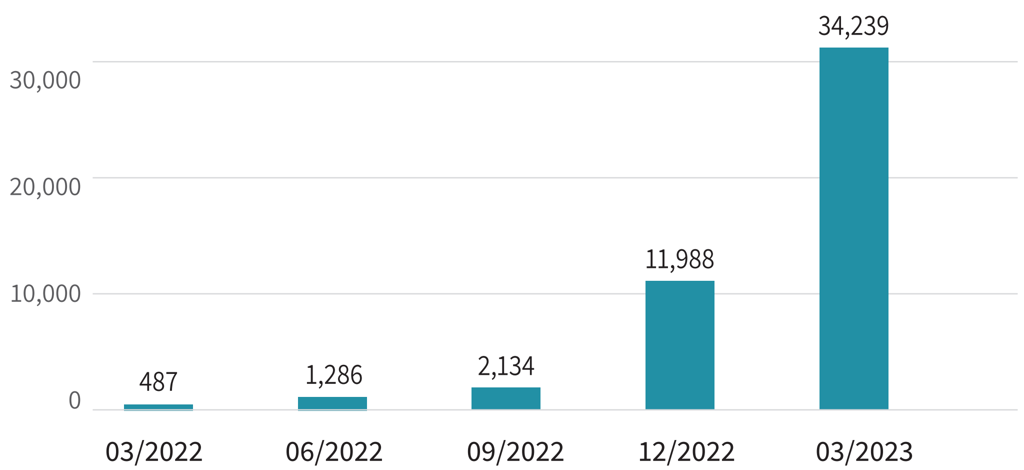
The development of the ecosystem and the implementation of open banking by the financial system requires collaboration between many players, including regulators and the participants: data sources, service providers and the customers themselves. Below we will describe the main challenges encountered in implementation:

13 Consent is defined as access permission—a data source will allow the customer to provide a service provider with permission to access his financial information that is located with the data source, by means of the interface system for financial information.

A uniform playing field

The law established a general regulatory framework for open banking activity and left it to the regulatory entities to fill in the details and to define its character and directives, the rules for data sources and service providers in a variety of areas, as well as coordinating among themselves in other areas. In addition to the cooperation needed between the various regulators, the regulatory complexity has created an additional challenge due to the need for regulation that will suit both a large organization, such as a bank or institutional entity, and smaller ones, such as fintech companies. In order to deal with this challenge, the Banking Supervision Department has worked to create a discourse with the staffs in the other regulatory entities, based on close cooperation that makes it possible to deal with the regulatory issues, in addition to the business and technological issues that relate to the entire ecosystem.

Figure 7.4 Number of Continuing Consents (end-of quarter balance), the Five Large Banking Groups, 2022:Q1–2023:Q1



SOURCE: Based on reports to the Banking Supervision Department.

Adoption of a standard that serves the entire system

The level of preparedness among service providers and among the entities receiving information is one of the challenges with which to deal. Thus, the Banking Supervision Department decided already in 2019 to establish an architects forum that is aimed at the fintech companies interested in operating as financial information service providers, as well as the ecosystem as a whole,[14] with the goal of clarifying issues related to the standard and responding to questions related to its implementation and assimilation in order to create an efficient ecosystem. Up until the passage of the law, the discussions on the forum centered on the business processes of open banking, the legislative process, and the date for going live. After the passage of the law, the forum centered on discussions of architecture issues and the changes required as a result of the law. Technical issues were brought up for discussion in the forum and there were sessions to explain the technological standard to all of the participants. This makes it possible for all of the players in the ecosystem to be ready when the system is launched.

Apart from the fact that the timetable established in the law was a challenge to the adoption of the technological standard, during the legislative stage the standard related to only two baskets of information, i.e., current accounts and payment cards, the domains that have been implemented in Europe. Thus, the Banking Supervision Department worked with the Berlin Group to establish an international standard, which did not previously exist, for the following information baskets: credit, deposits and securities. In practice, we had gotten ahead of Europe and there was a need to explain the activity in the Israeli market to the members of the Berlin Group and to write an international standard accordingly. An example of the complexity of activity in Israel relative to that in Europe is the various types of indexation for credit products and deposits that are not common in Europe.

Another challenge that has arisen in the implementation of the standard is the business and operational variation among the participants. The technology creates a significant degree of uniformity but since it is an international standard that can be applied in various markets, it provides degrees of freedom. Furthermore, there is variation across the data sources with respect to the character of their business activity and the manner in which their data is stored and in which it is presented to the customer in the digital platforms (apps and websites). These two factors create lacunae in the standard, and we, as the entity that is issuing the Israeli standard, had to define for the system participants the cases in which, despite the variation, a level of uniformity was required and the cases in which the variation should be preserved, based on the business issue and the circumstances.

[14] We invite fintech companies that are interested in operating as financial information service providers to join the architects' forum. An entity that is interested in taking part in discussions in the fintech companies forum is invited to submit its contact details together with half a page that describes its activity to: forumfintech@boi.org.il. These meetings are recording and uploaded to the Bank of Israel website as a service to the public. The address of the website: https://www.boi.org.il/roles/supervisionregulation/16992 [Hebrew]The draft proposes a delay in the application of the Securities Information Law until October 15, 2023 and a delay in the application of the requirement to provide access to data on the accounts of large corporations until April 14, 2024.

Practical implementation of the standard – initial difficulties and stabilization of the system

The open banking environment is a new system that is developing rapidly, and naturally there are issues that emerge from the work interfaces between the various parties that operate in the system. The Banking Supervision Department, which deals with each such issue in the immediate term, aspires to create a situation in which the response to an enquiry by a service provider and the investigation of system defects and their repair will be accomplished in a timely manner, as required in a system of this sort. This is reflected in the most recent version of Directive 368. The issues can be categorized as follows:

Understanding the technological standard – The Banking Supervision Department has responded according to the circumstances and either a localized solution was provided or if necessary a response was given in broader forums. In addition, if there was a need for further clarification, the subject was included in the FAQs that are published on the Bank of Israel website.[15]

Errors in the implementation of the standard – It appears that some of the errors are those of the service providers themselves, some are the result of incorrect implementation by the data sources, and others are the result of misunderstanding or an alternative interpretation of the standard by one of the parties. In these instances, the Banking Supervision Department has been in direct contact with the parties. If there was an error on the part of the service provider or the data source, they are asked to rectify it. If the standard was not implemented correctly (for example, if the data source or the service provider did not apply one of the compulsory fields appearing in the standard), then the responsible party is asked to operate according to the standard. This is based on the understanding that if the standard is not fully adopted by one of the sides then an effective response cannot be provided in accordance with the directive and the standard.

Information gaps in the standard – If there is information that is not dealt with clearly or correctly in the standard, we have acted to have the situation resolved, according the urgency of the situation. Further clarifications were added to the FAQs with regard to the lacunae in the standards until they are rectified. Note that as experience is accumulated in the system, the number of errors on the part of service providers and data sources diminishes.

[15] The FAQs can be found on the Bank of Israel website: https://www.boi.org.il/roles/supervisionregulation/16992 [Hebrew]

The future of open banking and global developments in the data sharing initiatives

The sharing of banking data by means of an open banking environment is only the first step in fully exploiting the potential. Even in processes of information sharing, open banking is only the first step toward an "open finance" system and eventually an open data system.

Uses of the open banking system

In order to maximize the ecosystem, the uses of the open banking environment can be expanded to those that do not appear in the law:

Expansion of payments in the open banking system – The world of open banking is divided into two arms—the reading of information and the writing of information. As mentioned, the Financial Information Services Law relates to the customer's access to information and its use. On the writing side, open banking in Israel and other countries focuses on the initiation of payments. The Ministry of Finance and the Ministry of Justice, together with the Bank of Israel, the Israel Securities Authority, the Capital Market Authority and the Competition Authority are currently in the process of formulating the Regulating Payment Services and Payment Initiation Law. As part of this legislation, the initiation of payments will be organized as it is in Europe, such that identification in order to create an authorization to debit an account is done with the payment initiator and—beyond what is the practice in Europe—will be expanded to advanced initiation (writing payment instructions for a customer on the basis of the customer's standing consent provided to the manager of his payment account). Accordingly, the Banking Supervision Department will expand the existing standard with respect to the initiation of payments to achieve a greater variety of services in this area, such as multiple payments, future payments, recurring payments, Request to Pay (RTP), etc. This activity will increase competition in the payments world, both between customers (P2P) and between customers and businesses (P2B), as well as expanding the inclusion of other means of payment, such as payment cards.

The Berlin Group is working to expand the standard for payments as part of the effort to strengthen the ecosystem of an open financial system and to add additional payment services to the standard. The Banking Supervision Department intends to work with the Berlin Group, which is seeking to expand writing not only in the case of payment instructions but also in the case of, for example, permission to debit an account, depositing into a deposit and even instructions for securities trading.

Open banking as an identification tool – The first stage for a client to join an open banking service is, as mentioned, strong identification of the customer by the data source, to enable him to create access permission. In other words, open banking has created a secure technological process in which the parties form a triangle: data source—customer—service provider. This process can also be used by the data source (a bank or credit card company) to identify a customer for other purposes that do not involve open banking. For example, the data source can offer customer identification services to various other entities (not necessarily financial ones, such as government entities, health services, etc.). In other words, in order to be identified through a third party, the customer is transferred to his bank or credit card company, where the identification process is executed (which is usually very fast, including a fingerprint), and he is then returned to the third party with a message from the bank or credit card company that the customer has been identified.

Open banking as a tool for improving the KYC process – Another use can be the transfer of information to a third party for KYC (Know Your Customer) or the onboarding of a customer at another financial body. The customer's consent can be obtained in the same way that he gives his consent to join open banking services. A customer begins the process with a third party, is transferred to his bank or credit card company that approves the transfer of the relevant information, and then is returned to the third party. This process can vastly improve the process for customers to connect with financial bodies, and in particular small and new ones, and can reduce the abandonment processes when the customer is required to submit forms as well as information that is not immediately accessible to him.

Advanced information sharing – an open finance system and an open data system

The global trend in the domain of information is expanding, such that the next steps in the data sharing sphere will cross from the world of finance to other domains. In other words, the customer will be able to provide existing information consumers (for example, financial information service providers or anyone else to be defined) with access to information other than his banking or financial information. This trend is expanding based on the approach that the customer's information belongs to the customer. Thus, the customer should be able to share information in other domains as well, such as with: infrastructure companies (gas, electricity and water), communication companies (cellular, Internet and television services) and local authorities.

Accordingly, a large number of countries have become active in the information sharing worlds, whether this effort is focused only on the sharing of limited banking information (open banking but only in payment accounts and credit cards) or broader sharing of information (open finance and open data).

There are market-driven initiatives in countries such as India, Japan, Singapore and South Korea, in which there is no regulation of open banking, although policy makers are promoting directives and rules to encourage open banking initiatives and information sharing. The US has also chosen a market-driven approach, but without any major government effort to support the development of open banking goods and services. The large banks in the US are well aware of the strategic importance of open banking and, in partnership with third parties, are developing API-based proposals as a way to attract new clients and achieve a competitive advantage.

In contrast, there are regulatory-driven initiatives in countries such as Hong Kong, Brazil, Australia, the EU, the UK, and Israel, which are more advanced than market-driven initiatives with respect to level of maturity and the information that is to be shared. Following are a number of examples:

One example is Australia, which is known for its innovative approach. The CDR regulation is not simply a financial services policy but is rather a policy for the sharing of data, such that the regulation will allow consumers to share not only their financial data but data in other domains as well. Although this will apply only to the banks at first, the regulation will apply at a later stage to the energy and communication sectors and eventually it will be possible to apply it in any sector.

Another example is Brazil, which serves as a major catalyst and is promoting the sharing of data on a large scale. This began with open banking, which developed into an open finance system and later was expanded to an open insurance system. It is planned that there will be interoperability between the two systems, such that entities in one domain will be able to receive information from entities in the other. In Brazil, the trend is also expanding to the sharing of health information. The Ministry of Health is initiating the creation of a platform for health information that will create unique medical information on a patient and will enable rapid mobility between the various health plans. The mechanism is being developed in partnership with the National Supplementary Health Agency (ANS) (which regulates the private-plans market), the Ministry of the Economy, and the central bank. The open health project is based on a similar approach to that of the open finance system. Namely, it will allow the sharing of data for the benefit of customers in health products and services. The main difference is in the sensitivity of information that will be shared. In the open finance system the data is financial (banking, insurance and investment) while in open health the data are health-related and have a higher level of sensitivity.

Europe has also adopted a strategy of opening up information in a large number of domains. This is based on the EU Data Act,[16] according to which many industries will be required to open up their data.

As described, there are many open banking initiatives. The following table compares a number of open banking and data sharing initiatives to open banking in Israel:

	Israel	**UK**	**Europe**	**Brazil**	**Australia**
Scope of information	Financial Information Service Law: payment accounts; credit cards, deposits; securities	Payment accounts[17]	PSD2 Payment accounts; debit card accounts	Open finance,[18] open insurance,[19,20] and open health[21]	Open finance[22]
Sector	Financial	Banking	Banking	Financial (including insurance)	Financial, infrastructure, communication
Extent of access	Read - writing	Read - writing	Read - writing	Read - write and writing (there is payment initiation)	Read only
Definition of the standard	Bank of Israel	OBIE – The regulatory bodies created an entity financed by the industries.	Various initiatives	The central bank	CDR – a government body

16 https://www.eu-data-act.com

17 https://standards.openbanking.org.uk/customer-experience-guidelines/account-information-services/latest

18 https://liftchallenge.bcb.gov.br/en/financialstability/open_finance

19 https://thepaypers.com/online-mobile-banking/brazil-rolls-out-phase-2-of-open-insurance--1261580?utm_source=newsletter&utm_medium=email&utm_campaign=Daily+2023-03-01+Daily-Newsletter-Banking

20 https://www.openbankingexcellence.org/blog/open-insurance-in-brazil

21 https://thepaypers.com/online-mobile-banking/open-banking-inspiration-brazil-to-enter-open-.health—1257797

22 https://www.cdr.gov.au/rollout

The sharing of information in the banking system is, according to the Bank of Israel, only the first step and efforts should continue to share financial data from all sources in the Israeli ecosystem, with the goal of allowing customers to obtain a full picture of their financial activity. As mentioned, the Financial Information Services Law specifies that institutional entities with a license to provide deposit and credit services[23] will also serve as data sources in the case of the relevant information baskets.

There is financial data located with additional financial entities that at this stage are not required to share it in open banking. Furthermore, there are additional entities that are not required at all to serve as data sources (such as members of the stock exchange and brokers). However, the Minister of Finance has the authority to require these entities to operate in the ecosystem and with respect to additional information (financial data such as long-term savings (provident funds and pensions)). The opening of the entire system to the sharing of information will enable customers to view the entire picture of their financial situation in one place. That is, from a consumer perspective, customers will have an overall (and objective) view of all their information, such that the advantages of open banking will be copied to products in other domains (including reduced costs, value proposals, full aggregation services, etc.). The full picture involves more than just the presentation of full information, it achieves a synergy between the products. For example, if the amount of a mortgage changes, the financial information service will be able to determine whether the customer's life insurance is still sufficient, and if not, it will be possible to suggest to the customer that he change his insurance coverage. Another example could be a one-time transfer of funds (closing of a mortgage track) or periodic transfers (periodically depositing into a provident fund) in which the receiving entity can streamline the customer's processes—first by initiating a single or periodic payment and subsequently in all of the verification processes with the payer. In this way, it is possible to eliminate unnecessary friction and abandonment by the customer when carrying out financial activities.

Business management is changing and becoming increasingly data-based. However, it is important not only to obtain information but also to know how to analyze it, make wise use of it, and offer interesting services and ideas. The success of open banking has increased the appetite and desire for information to be opened up in many other domains and that the various domains be connected in order to maximize the added value for consumers. The integration of information from various domains can expand the insights and added value of the customer and will lead to economic growth, on both the individual and economy-wide levels. In 2018, it was estimated that in the UK information sharing and the models that

[23] An entity with a license to provide deposit and credit services as defined in the Control of Financial Services Law.

would develop as a result would contribute about 27.8 billion pounds per year to the British economy[24] and it is estimated that the contribution to GDP will be about 1.15 percent in 2030.[25]

In addition, in January 2021, a joint paper[26] was published by the Privacy Protection Authority (a unit in the Ministry of Justice), the Competition Authority and the Consumer Protection and Fair Trade Authority, recommending that legislation be adopted to establish the right of information mobility. The document relates to the increase in the volume of data and the fact that the use of consumer data leads to the development of new products, services and business models, and finally that changes are needed in Israeli law in order to provide the consumer with the right of information mobility. The advantages to the consumer and the Israeli market from the adoption of this right are significant: providing the individual with control over the personal information that has been gathered by various entities, given that he has the rights over that information; providing the possibility of transferring personal information between suppliers so as to reduce the cost of moving in the various domains and increasing the competitive pressure from small or new companies on companies that control the market; and the empowerment of the consumer vis-à-vis large organizations, as well as improving the service provided and the user experience. However, in order to ensure that this right will have an impact and will achieve its goals, it should be formulated with care.

[24] From: Data mobility: The personal data portability growth opportunity for the UK economy, 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/ Data_Mobility_report.pdf

[25] https://www.mckinsey.com/industries/financial-services/our-insights/financial-data-unbound-the-value-of-open-data-for-individuals-and-institutions

[26] https://www.gov.il/BlobFolder/policy/dataportability/he/opinion.pdf

Box 7.2
Regulating the banking corporations' activity in crypto assets

- Recent years have seen increased activity in financial crypto assets both in Israel and worldwide.
- There are numerous risks implicit within crypto asset activity, some of which have been realized during the past year; nonetheless, these financial instruments also have the potential for innovation in the financial world.
- Among the risks existing in crypto asset activity are compliance risk, money laundering and financing of terror (ML/FT) risk, credit risk, legal risk, market and liquidity risk, technological risk, operational risk, fraud and embezzlement risk, risks to the stability of the financial system and risks related to the relations between the bank and its customers.
- In recent years, we have seen the development of both global and domestic regulation, with the goal of wisely managing these risks.
- With respect to domestic banking regulation, several amendments have been made during the past year to Proper Conduct of Banking Business directives, with the following goals:

  1) To regulate payment services that are provided as a result of activity in virtual currencies (namely, the deposit and transfer of funds that originate in investment in virtual assets);

  2) To regulate the possibility of the banks offering new products to customers in the area of crypto assets.

  These amendments were required following the changes in regulation carried out by parallel supervisory authorities, in particular the applying of the Prohibition on Money Laundering Order to financial service providers in the crypto domain in Israel.

- The Banking Supervision Department will continue to monitor the developments in crypto assets and will work toward increasing benefit to the customer, including the careful management of risk in order to protect the banking system and its customers.

In recent years, we have been witness to increased activity in financial crypto assets,[1] both in Israel and worldwide. Among other things, new and innovative assets and services are

[1] The term "crypto asset" in general refers to any digital asset that is based on cryptographic technology. The term "crypto-related activity" includes the issuing of crypto and other digital assets; custody services for crypto assets; holding of stablecoin reserves; buying and selling of cryptographic currencies; activity as a clearing house; credit activity based on crypto; and innovative related activities that will emerge in the future.

being developed by a variety of players and they are increasingly being offered to the public. The involvement of the banking corporations and merchant acquirers in related activities, whether directly or indirectly, may have an impact on the ability to ensure a stable and trustworthy financial environment.

Activity in crypto assets involves numerous risks, some of which have been realized during the past year; nonetheless, these financial instruments also have the potential for innovation in the financial world, since they have the ability to improve the execution of financial activity and reduce the costs of a transaction, eliminate the need for intermediaries, and provide alternative methods of payment to those without access to regular financial products and therefore increase financial inclusion.

Over the years, the banking corporations have adopted a cautious approach to anything connected to activity in crypto assets and have avoided offering products that rely on these assets. Furthermore, they have adopted a policy of caution with regard to the acceptance of funds that originate in crypto asset activity (whether payment services that accompany activity in these currencies or investment activity); neither have they invested in such assets directly. This approach is the result of the high level of risk implicit in virtual assets activity[2] (where some of the risks have been realized even in the last year). It is also a result of the fact that these are new activities that are developing rapidly and as such, they are still not familiar and fully understood, thus magnifying the risks and concerns surrounding this activity. This is especially true given that regulation has not yet been modified to include this type of activity. Nonetheless, we note that in view of the developments in global markets and the changes in the relevant regulation, we are currently seeing some crypto services being offered by a number of Israeli banks and credit card companies.

In recent years, there have been developments in both global and domestic regulation, the goal of which is to facilitate the activity in crypto assets, based on wise management of these assets. The current legal and regulatory environment is not encouraging nor prohibiting the banking corporations from allowing their customers to carry out various activities in crypto currencies. Nonetheless, it is essential that any activity related to cryptographic assets offered by the bank to its customers, including the provision of payment services connected to activity in virtual currencies, will be provided with the necessary caution and will be based on ensuring the stability of the corporations, protecting the customer and maintaining fairness, as well as compliance with the law and existing regulation, particularly with regard to AML/CFT.

[2] A digital representation of a financial asset that is referred to in various ways, including crypto currencies, virtual currencies, digital assets, etc. For our purposes all of these terms, as they appear in this box, relate in general to the same activity.

With respect to local banking regulation, several amendments have been made to the Proper Conduct of Banking Business directives, with the following objectives:

(1) To regulate payment services connected to activity in virtual currencies (namely, the deposit and transfer of funds that originate in investment in virtual assets);

(2) To establish the obligations of the banks in the event that new products are offered to customers in the space of crypto assets.

It became possible to promote these amendments after developments in global regulation and regulatory changes carried out by parallel supervisory authorities in Israel and in particular the application of the Prohibition on Money Laundering Order on virtual asset service providers.

The risks to the banking system that are implicit in crypto assets activity

The activity in crypto assets creates both microeconomic and macroeconomic risks for the banking system. With regard to the former, which are liable to have an impact on the stability of the banking corporation itself, there is a long list of risks, which also include traditional financial risks. A major risk in the context of crypto asset activity is compliance risk. This is due to the fact that this activity is often connected to ML/FT activity, since these platforms can be used for cross-border transfers of large sums, while taking advantage of the inherent anonymity that is an integral part of some of these currencies and in many cases the lack of mediation by financial bodies to which the AML/CFT regime applies. In general, there are reported cases of the use of crypto assets for illegal activities, in view of the difficulty in tracing the source of the funds and identifying the owners. This is certainly true when there is a fundamental difficulty in verifying and proving ownership in a formal and validated manner, particularly in a rapidly developing environment.

In addition, various activities in crypto assets are liable to create credit risk, market risk and liquidity risk in the banking system. There is concern about exposure to credit risk originating from a crypto asset or the structure in which it is held, which derives from the difficulty in measuring the asset's quality and fair value, the possibility of the its being realized, and from exposure to counterparty credit risk. The issue also derives from the difficulty in determining whether the asset is bankable. There is significant market risk due to the doubt as to whether there are appropriate ways to price and assess the value of crypto assets. Moreover, the standards for accounting treatment and financial reporting for crypto assets and crypto-related activity are still evolving and are likely to have a significant effect on all parties involved, including the impact on the allocation of capital[3] due to this activity, up to the point of not being worthwhile from a business aspect. There is also liquidity risk, particularly in the case of the most volatile crypto assets.

In addition to the aforementioned, there are technological risks that challenge the existing protection mechanisms. These involve the level of risk, the protection of privacy, the integrity and accessibility of information systems and information assets. There are also operational risks that are the result of relationships between the banking corporations and third parties, such as entities that specialize in crypto, which are not supervised and whose management and corporate governance mechanisms are still in the early stages of development.

It is also worth noting that the unique characteristics of cryptographic assets, particularly the reliance on third parties, are liable to constitute fertile ground for fraud, embezzlement and trade manipulation, in addition to the risks to information systems, information security and the Internet environment, such as the theft or loss of personal keys (passwords) and cyber attacks on crypto asset exchanges.

Alongside the macroprudential risks, certain crypto assets and related activities are also liable to create systemic risks that are unintentionally generated by the structure of activity in these assets or in light of the interplay between activities in crypto and the traditional financial system. In addition, disruption or fraud in activity related to crypto assets is liable to create a run on financial assets that back up the crypto asset or crypto-related activity and thus lead to a self-generating cyclical movement in the redemption of financial assets and fire sales, which itself is likely to critically disrupt financial markets and may lead to a risk of contagion. Moreover, operational failures such as fraud and embezzlement, trade manipulations and cyber attacks that are linked to crypto assets or to related activities are liable to have a destabilizing impact on corporations active in this domain.

It is also worth mentioning behavioral risk as one of the risks implicit in this activity. The Banking Supervision Department is aware of the consumer risks that are the result of new activities in the crypto space, such as customers' lack of familiarity with the crypto assets being offered by the banking corporations. An example is the risk implicit in the speculative nature of certain crypto assets relative to traditional banking products, such as deposits. In addition, customers are likely not to understand the role of the banking corporation in this activity and to place the same level of trust in the activity as they do in the banking corporation. In addition, the banking corporation is dealing with compliance risk in the context of implementing consumer directives, such as appropriate, clear and broad disclosure

[3] The BIS Committee on Banking Supervision published a document in December 2022 that established rules for the allocation of capital in cryptographic asset services (Prudential Treatment of Crypto Assets Exposures). Parallel directives have not yet been published in Israel. https://www.bis.org/bcbs/publ/d545.htm

formulated in clear and simple language so that customers will properly understand the risks, as well as directives related to marketing techniques and practices that are misleading or are liable to mislead. Finally, we would stress that the realization of some of the aforementioned risks is liable to constitute a risk to the banking corporation's reputation.

In view of this array of risks and in particular the failure events worldwide in the crypto space during the past year—including, among others, the crash of the Terra-Luna currencies and the FTX Exchange—the Supervisor of Banks distributed a letter to the CEOs of the banking corporations and credit card companies that describes the main risks implicit in crypto activity, as many supervisory authorities have done worldwide.[4]

Regulating the providers of services in virtual currencies

The global regulation in this space is in its early stages. Countries worldwide are in different stages of creating a regulatory framework for the domain of virtual assets. In June 2019, the Financial Action Task Force (FATF) approved the amendment of international standards regarding AML in virtual assets and published a guide[5] to help countries implement the organization's recommendations. According to the recommendations, each of the member countries is obligated to implement AML/CFT regulation with respect to activity in virtual assets and virtual asset service providers (VASPs). According to these standards, countries are obligated to assess the risks implicit in this activity, and service providers must take measures to mitigate them. In addition, countries are required to impose a licensing or registration obligation on providers of services in this space. Furthermore, VASPs will be under the supervision of an entity with the relevant authority, including the power to carry out audits, obtain information and impose sanctions in the case that service providers do not fulfil their AML/CFT obligations. A country must ensure that the service providers will evaluate the AML/CFT risk and will carry out a check of their customers, will keep records and will report on suspicious transactions as required of entities that are subject to AML/FT regulation.

The FATF's periodic surveys of the activity in virtual assets indicate that although various member countries are making progress in the implementation of the organization's recommendations regarding activity in this domain, the performance of most countries still needs to be improved (and in some cases, a great deal of improvement is needed). The most common shortfalls in implementation include: legislative measures as part of the

[4] See the letter from the Supervisor of Banks on "Dealings in financial cryptographic assets" dated February 26, 2023. https://www.BankofIsrael.org.il/media/m2lp4mbj/202314_en.pdf

[5] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, June 2019.

implementation of the Travel Rule, i.e., FATF requirements for the registration and submitting of identifying details for parties in the transfer of virtual assets; gaps in the assessment of AML/CFT risk; implementation of preventative measures and enforcement tools; and the accelerated implementation of the organization's recommendations in general. The narrowing of these gaps will help achieve an effective global regime for virtual assets and VASPs.[6]

In a document published in 2021, the BIS's assessment was that the supervision of VASPs on a global level is in its early stages. Most of the countries are in the initial stages of implementation and enforcement of the international AML/CFT guidelines and steps have not yet been taken to implement active supervision of VASP activity.[7] In January 2023, the organization published another paper, which included a discussion of the possibilities facing regulatory bodies in order to regulate this activity.

The paper described three approaches to the regulation of activity in cryptographic assets and their advantages and disadvantages:

(1) To prohibit activity in crypto;

(2) To isolate crypto activity from the traditional economy;

(3) To regulate crypto activity like the traditional economy.

In the paper, the BIS also presents an alternative that would create an infrastructure to encourage and facilitate stable innovation in the domain, which will serve to improve the traditional economy.[8]

In **Israel**, the regulatory body for VASPs is the Capital Market Authority. In 2016, the Control of Financial Services (Regulated Financial Services) Law, 5776–2016, was passed. It established that the Commissioner for the Capital Market, Insurance and Savings would serve as the supervisor over providers of financial services that are not banks or institutional bodies. These services include, among others, the purchase, sale, conversion, exchange, transfer, storage and management of financial assets, including virtual currencies that are defined in the law as a "financial asset". The law added the financial service providers to the list of entities included in the Third Addendum to the Prohibition on Money Laundering Law, 5760–2000, to

[6] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2022; Second 12-Month Review of the Revised FATF Standards – Virtual assets and VASPs, July Month Review – Revised FATF Standards on Virtual Assets and VASPs, June 2020; 2021 12.

[7] FSI Insights on policy implementation No. 31 Supervising cryptoassets for antimony laundering, April 2021.

[8] Aquilina, Matteo, Jon Frost and Andreas Schrimpf. Addressing the risks in crypto: laying out the options. No. 66. Bank for International Settlements, 2023. https://www.bis.org/publ/bisbull66.pdf

which the AML/CFT regime applies. The Money Laundering (Obligations for Identification, Reporting and Management of Records for Providers of Service in a Financial Asset and Providers of Credit Services for the Prevention of Money Laundering and Financing of Terror) Order, 5778–2018, was amended in order to impose AML/CFT obligations on providers of services in a financial asset (including VASPs); it went into effect in November 2021. This represents another stage in the mitigation of risk to the banking system in the management of this activity. Additional components, as required by the international standards in this context, will constitute the basis for the supervision and enforcement imposed on these bodies and the imposition of the obligation incumbent on VASPs to submit identifying details of entities carrying out activity in virtual currencies.

In this context, and despite the progress in regulation in recent years, the National Risk Assessment of AML/CFT risk carried out in November 2021 ranked providers of currency services that operate in risk domains (such as crypto), as high-risk (4.5 out of 5).[9]

All of the financial regulators in Israel share the philosophy that further progress should be made in the regulation of digital assets, and that in this context interministerial coordination and cooperation is necessary. As part of this approach, the Chief Economist of the Ministry of Finance published a report in November 2022 on the regulation of digital assets.[10] It provides a survey of the regulatory picture for these assets in Israel and worldwide, guidelines for regulation in the domain, and policy recommendations for all of the relevant bodies in the Israeli economy. The recommendations primarily have to do with the removal of barriers while maintaining the necessary risk management, regulation and expansion of existing powers, the concentration of authority in one entity, and anchoring of the licensing power in law, as well as supervision over stablecoins and the provision of financial services that make use of them.

During the past two years, a Bank of Israel committee headed by the Deputy Governor has been examining various aspects of digital assets: regulatory, technological, monetary and legal. Among other things, the committee formulated a document of guidelines for the regulation of activity in stablecoins in Israel, which was published in February 2023.[11] The goals of regulation are to enable activity in stablecoins while managing the risks implicit in their use and to modify consumer protection and prudential obligations so as to facilitate this unique activity.

[9] Israel Money Laundering and Terror Financing Prohibition Authority, "National Risk Assessment for the Prohibition of Money Laundering – Enforcement Bodies", November 2021. https://www.gov.il/blobFolder/dynamiccollectorresultitem/nra-enforcement-bodies-2021/he/periodic-docs_nra_enforcement_bodies_2021.pdf [Hebrew]

[10] The Chief Economist of the Ministry of Finance, "Report on the Regulation of Digital Assets – A Policy Roadmap", November 2022. [Hebrew]

[11] Bank of Israel - Principles for Stablecoin activity, February 2023

The changes in Israeli banking regulations as they relate to crypto assets

During this past year, the Banking Supervision Department made two amendments to the Proper Conduct of Banking Business directives with the goal of regulating the activity of the bank and its customers in the area of crypto assets.

The **first amendment** concerns payment services for the bank's customers related to their activity in virtual currencies. In view of the increasing scope of activity in virtual currencies and as a result of the increase in requests by customers to transfer funds that originate in this activity to their payment accounts in the banking system, in May 2022 the Banking Supervision Department amended Proper Conduct of Banking Business Directive 411, which deals with the management of AML/CFT risk. The amendment added Section 87a to the directive, which deals with payment services related to activity in a virtual currency.[12]

The directive defines the guidelines for management of AML/CFT risk that is the result of the aforementioned activity and establishes that banking corporations must make a specific assessment of the relevant risk. Furthermore, a banking corporation will not refuse to provide payment services related to activity in a virtual currency only because virtual currencies are involved, provided that the VASP that is a side in the transaction has obtained a service provider license in Israel. In addition, the directive defines, among other things, several areas that are to be included in the policy and procedures to be decided on in the assessment of risk carried out by the banking corporation, which will be based on a risk-based approach. Among other things, the identity of the service provider should be investigated as well as the AML/CFT requirements that apply to his activity. The directive prohibits a sweeping policy of refusal in the case of activity carried out in a virtual currency by a service provider who has obtained a license from the Capital Market, Insurance and Savings Commissioner to provide services in a virtual currency. In addition, the banking corporations are required to formulate a policy with respect to their activity carried out by way of other providers of services in virtual currencies, based on the findings of a risk survey they have carried out. The directive establishes that the banking corporation is to determine the virtual currency channels in which it will permit payment services related to activity in a virtual currency. It will also ascertain the source of the funds used to purchase the virtual currency and the route the funds have taken from the time of the purchase of the virtual currency until the deposit of the funds originating in the sale of the virtual currency into the customer's account at the banking corporation.

[12] Proper Conduct of Banking Business Directive no. 411 on Management of Anti-Money Laundering and Countering Financing of Terrorism Risks https://boi.org.il/media/lecnlar1/411_et.pdf

In addition, the directive includes a requirement of disclosure to the customer, according to which the customer is to be informed of the banking corporation's policy regarding the receipt of funds originating in activity in virtual currencies from a provider of services in a virtual currency in an account managed at the banking corporation. This is to be done by way of all of the possible channels for carrying out the activity (at the branch, by telephone, using an app, etc.) near the time of—and if possible prior to—the first transfer from the account at the banking corporation to the account of the provider of services in a virtual currency. Finally, the banking corporation is required to publish its policy regarding the provisiding of payment services related to activity in virtual currencies on its website.

The **second amendment** relates to new products that are offered to customers by the bank in the domain of crypto assets. In February 2023, the Banking Supervision Department published a revision of Proper Conduct of Banking Business Directive no. 310 on Risk Management, which draws attention to the derived risks in this domain, including consumer-oriented requirements related to this activity.[13] As part of the amendment to the directive, the requirements that apply to the process of offering a new product to the bank's customers were expanded, such that the process will also include a check that the product meets the relevant laws and regulations, and that the assessment of risk will examine the bank's obligations toward its customers. Furthermore, given the potential risk implicit in activity related to crypto assets, an obligation was established to notify the Supervisor of Banks ahead of time and in writing of activities related to crypto assets.

The Banking Supervision Department will continue to track the developments in the domain of crypto assets and will continue its efforts on behalf of customers, including the careful management of risk. In addition, it intends to anchor in law the directives for periodic reporting to the Banking Supervision Department with respect to the scope of transfers and deposits of funds resulting from activity in virtual currencies and with respect to the scope of account openings and account management of customers that are VASPs.

[13] Proper Conduct of Banking Business Directive no. 310 – Risk Management.
https://boi.org.il/media/mfzpi0dn/310_et.pdf

Box 7.3
Payment of salaries by means of bank transfer to Palestinian workers legally employed in Israel

- During the past two years, there has been a collaborative effort led by the Accountant General's Division in the Ministry of Finance, together with the Bank of Israel, the Coordinator of Government Activities in the Territories, and the Population and Immigration Authority to create a mechanism for paying the salaries of Palestinian workers legally employed in Israel who are residents of Judea and Samaria, by means of bank transfer to their accounts, following verification of their employment in the official database.
- This mechanism will provide the banks with access to the Population and Immigration Authority's official registry, which includes information on Palestinian employees. The verification of information on Palestinian employees using Israel's official database will significantly reduce the risk of money laundering and financing of terror since the process will confirm the legality of the employment and that the security services have no indication of the worker's involvement in terrorism.
- At the end of 2022, the banking system's preparations to receive information from the Population and Immigration Authority were completed. This will enable the payment of salaries by means of bank transfer on a large scale. Furthermore, in the beginning of 2023, the Population and Immigration Authority imposed an obligation on Israeli employers to pay the salaries of their Palestinian workers working in Israel by means of bank transfer to their accounts in the Palestinian Authority (PA).
- The transition to salary payments by means of bank transfer will help to reduce the use of cash and as result will contribute to eliminating money laundering and tax evasion in Israel. Furthermore, it will improve the supervision and control capabilities of the Israeli authorities with respect to the salaries paid to Palestinian workers.

Background

There are currently about 120,000 Palestinian workers employed in the State of Israel and according to estimates, the amount of cash paid to these workers each year is about NIS 10–15 billion.

The widespread use of cash facilitates tax evasion, money laundering, the financing of terrorism, and various other violations of the law. It also makes it possible to circumvent the financial system, which serves as an important gatekeeper in the fight against money laundering and the financing of terror. In view of these undesirable phenomena, the Reducing the Use of Cash Law, 5778–2018, was passed. Its goal is to limit the use of cash, and based on this law, limits were imposed on the payment or receipt of salaries in cash.[1]

The payment of salaries in cash to Palestinian workers creates several additional challenges, such as the difficulty in supervising the payments and maintaining control over the payment of taxes to Israel and the PA. It also sometimes results in disagreements between Palestinian workers and their employers over the amount of salary actually paid. The widespread use of cash has adverse consequences on the PA's side as well. In discussions with representatives of the Palestine Monetary Authority, the IMF, and other international organizations, it became clear that the payment of salaries by means of bank transfers to the bank accounts of the workers in the PA will help to reduce the amount of cash handled by the banks operating in the PA and will reduce operating costs significantly, alongside the improvement in financial inclusion.

Government Decision 2174 in December 2016 with respect to the scope of employment of Palestinian workers from Judea and Samaria in Israel, the improvement in allocation of work permits and ensuring fair employment conditions for Palestinian workers was a major step in dealing with these and other challenges. As part of this decision, it was decided, among other things, that a joint workgroup would be created with the goal of examining the arrangements for the payment of salaries and social benefits to Palestinian workers, including the obligation of employers to transfer their salaries directly into their bank accounts by means of a mechanism to be decided on by the workgroup. The workgroup was headed by the Director General of the Ministry of Finance, and it decided to recommend a mechanism for the payment of salaries to Palestinian workers using bank transfers. In order to implement the decision, there was a joint study led by the Accountant General's Division in the Ministry of Finance, together with the Bank of Israel, the Coordinator of Government Activities in the Territories, and the Population and Immigration Authority with the goal of creating a mechanism that would enable the payment of Palestinian workers who are residents of Judea and Samaria and who work legally in Israel by means of bank transfers to their accounts in the PA.

At the end of the study, the Population and Immigration Authority notified Israeli employers of the creation of the mechanism and the requirement, starting from January 1, 2023, to pay the salaries of Palestinian workers who are residents of Judea and Samaria by means of a bank transfer to their bank account in the PA.[2]

[1] In the case that the salary exceeds NIS 6,000 (Section 2 of the law). An exemption was granted by temporary order to Israeli citizens who pay cash to residents of Judea and Samaria or to residents of the Palestinian Authority who are not Israeli citizens or someone who receives payment in cash from those same residents.

[2] Circular of the Civilian Authority 18/2022 from November 2, 2022 of the Population and Immigration Authority concerning "The obligation to pay Palestinian workers by means of a bank transfer". https://www.gov.il/he/Departments/policies/obligation_to_pay_palestinian_workers [Hebrew]

Payment of salaries to PA workers prior to the creation of the mechanism

Prior to the creation of the mechanism, employers were able to pay salaries to their Palestinian workers legally employed in Israel by mean of bank transfer, but it was a complex process from the side of the banks, given the demands of the AML/CFT regulations. It involved a check of each transfer, making it difficult to carry out bank transfers on a large scale and in a timely manner. This problem was exacerbated by the fact that the PA is defined as a high-risk territory with respect to AML/CFT, which requires expanded monitoring of financial activity with the PA and reporting to the Authority for the Prohibition of Money Laundering and Finance of Terror at much lower thresholds than in the case of countries that are not defined as high-risk territories.

Therefore, to facilitate the routine payment of salaries by way of bank transfer to all Palestinian workers employed with a permit, it was necessary to ensure that the banking system would have accessible and efficient tools to manage the risk. In this way, the transfers could be made in a user-friendly and efficient manner. Thus, there was a need to provide the banks with access to the State's official registry, which includes information on Palestinian employees. The Banking Supervision Department's approach was that the verification of information about Palestinian employees using the State's official database would significantly reduce the AML/CFT risk since it would confirm the legality of employing the worker and that the security services have no indication of his involvement in terror.

Creation of the mechanism and its use

The mechanism that was created by the interministerial workgroup includes a system that can be used to verify the details of the employee against the Population and Immigration Authority's system. In order to implement the mechanism, it is required that each Palestinian worker provide his consent that the bank carrying out the transfer will verify the legality of his employment with the Population and Immigration Authority. The worker's consent is a condition for the Civilian Authority to grant him a permit to work in Israel.[3]

In parallel, the Banking Supervision Department considered the various channels by which the salaries could be paid to Palestinian workers to streamline the process. It worked to achieve a situation in which the payment could be made by direct means (such as the Internet) or by telephone, in addition to the possibility of transfers by means of a teller at a bank branch.

[3] Circular of the Civilian Authority 9/2022 from August 1, 2022 of the Population and Immigration Authority concerning "Revision with regard to the creation of a mechanism for paying the salaries of Palestinian worker by means of bank transfer". https://www.gov.il/he/departments/policies/payment_palestinian_worker [Hebrew]

As a complementary measure, the Supervisor of Banks issued a circular to the CEOs of the banks in June 2022 concerning "The payment of salaries to Palestinian workers by means of bank transfer".[4] It stated that when carrying out a bank transfer to pay the salary of a Palestinian worker, the information on the worker is to be verified against the information that will be accessed from the database of the Population Authority and that this process will replace the verification required by the Prohibition on Money Laundering Order.[5] Accordingly, the Banking Supervision Department amended Proper Conduct of Banking Business Directive no. 411 on Management of Anti-Money Laundering and Countering Financing of Terrorism Risks, which established, among other things, that the implementation of salary payments to Palestinian workers by means of bank transfers will be according to that circular.[6]

On November 2, 2022, the banking system's preparations to use the information from the Population Authority's database were complete and it was ready to carry out salary payments by means of bank transfer on a large scale. At a later stage, the Population and Immigration Authority made it mandatory for employers to pay the salaries of Palestinian workers by bank transfer starting from January 1, 2023.[7]

All of the entities involved are continuing to monitor the use of the mechanism and the scope of the salary payments carried out by bank transfer, and they are considering the possibility of expanding the process if necessary.

The transition to salary payments by means of bank transfer will help to reduce the use of cash and as a result will contribute to eliminating money laundering and tax evasion in Israel. Furthermore, it will improve the supervision and control capabilities of the authorities in Israel with respect to the salaries paid to Palestinian workers. This step will also reduce the use of cash in the PA and will encourage the financial inclusion of PA residents, as well as increasing the efficiency of the economic system.

[4] Circular no. 2712 of the Banking Supervision Department, June 30, 2022 concerning "Payment of salaries to Palestinian workers by bank transfer". https://www.boi.org.il/en/economic-roles/supervision-and-regulation/2527/wage-payments-to-palestinian-workers-via-bank-transfers-30062022/

[5] This verification is required by Section 13a(3)(b) of the Prohibition on Money Laundering (Obligation to identify, report and manage the records of the banking corporations in order to prevent money laundering and the financing of terror) Order, 5761.

[6] Proper Conduct of Banking Business Directive no. 411 – Management of Anti-Money Laundering and Countering Financing of Terrorism. https://boi.org.il/media/lecnlar1/411_et.pdf

[7] Circular of the Civilian Authority 18/2022 from November 2, 2022 of the Population and Immigration Authority concerning "The obligation to pay Palestinian Workers by means of a bank transfer".
https://www.gov.il/he/Departments/policies/obligation_to_pay_palestinian_workers

Box 7.4
The activity of the Banking Supervision Department with regard to the Russia-Ukraine war

- Given the importance it attributes to providing optimal-quality banking service to new immigrants, the Banking Supervision Department is working by various means to allow new immigrants to optimally manage their banking and financial activity.
- In light of the important role of the financial system in the lives of new immigrants, the Banking Supervision Department has worked and will continue to make an effort in a variety of ways to help this population deal with the problems they encounter in the Israeli banking system. This is with an emphasis on their sensitive treatment by the banking system and providing them with access to banking services.
- As a result of the Russia-Ukraine war, various countries and international organizations have adopted a regime of sanctions against various entities with respect to activity with Russia. The war has led to an increase in the risk of money laundering and financing of terror (AML/CFT) in activity interactions with Russia. Thus, the potential that the banking system will be exploited in order to circumvent these sanctions exposes the banking corporations to significant risks, including compliance risk and AML/CFT risk.
- The banking corporations in Israel face numerous challenges in finding a balance between the importance of managing the various risks they face and that of providing services to new and existing customers.

Background

The war between Russia and Ukraine, which began in February 2022 and is still ongoing, has led to the imposing of sanctions by advanced economies against Russia. The war also led to a large increase in the number of new immigrants from FSU countries (Ukraine, Russia, and Belarus) who are seeking to make Israel the center of their lives.

As a result of the war, various countries and international organizations have created a complex and dynamic regime of sanctions, which has consequences for individuals, businesses, financial entities, geographic areas, and various sectors of the economy.

The potential exploitation of the banking system in order to circumvent these sanctions exposes the banking corporations to major risks, including compliance risk, AML/CFT risk, legal risk, and reputational risk.

As a result of the war, the banking corporations in Israel are facing numerous challenges in maintaining a balance between two regulatory obligations: the management of risk given the significant exposure to a violation or circumvention of international sanctions, while at the same time there is the obligation to provide service to customers, which includes providing new immigrants with the possibility of managing their finances in Israel.

In view of the importance of the financial system in the lives of new immigrants, the Banking Supervision Department has used and will continue to use a variety of means to assist this population. The main message to the banking system is to provide an optimal level of service to new immigrants, with emphasis on sensitive treatment and accessibility to services in the Russian language, subject to the banks' risk management policy.

The main activities of the Banking Supervision Department:

Regulatory activity

Since the outbreak of the war, the Banking Supervision Department has distributed three letters to the banking corporations that instruct them to manage the risk of exposure to exploitation for the purpose of violating or circumventing international sanctions and to operate with caution and sensitivity to the situation of existing and new customers who are affected by the war.

1. The letter from the Supervisor of Banks dated June 8, 2022 on "The risks implicit in relations with entities appearing on the international sanctions lists and national sanctions lists of foreign countries" required the banks to establish policies and procedures for the way in which they use the international and national lists of sanctions and with respect to their relationships or execution of transactions with entities appearing on those lists, as part of the risk management process incumbent on them and within the context of complying with Proper Conduct of Banking Business Directive no. 310, on Risk Management. This is subject to the obligations of the banking corporations toward their customers while taking into consideration the circumstances and the nature of the activity. The letter also emphasized that refusing to carry out an action, to form a new relationship or to end an existing one due to the implementation of the aforementioned policy will be viewed as a reasonable refusal to provide service according to the Banking (Service to the Customer) Law, 5741–1981.
2. The letter from the Supervisor of Banks dated August 16, 2022 on "The opening of an account for new immigrants and receipt of funds from Russia through the banking system in Israel" emphasized the Banking Supervision Department's expectation that an optimal level of service will be provided to new immigrants by the Israeli banking

system, with emphasis on sensitivity to their situation, including providing access to basic banking services in the various channels of operations in the Russian language and the standardization of work processes across a bank's various branches.

3. The letter from the Supervisor of Banks dated February 2, 2023 on "Providing service to customers in the Israeli banking system against the background of the Russia-Ukraine war" was in response to enquiries from social organizations and the banking system's customers regarding the difficulties encountered by new immigrants in the Israeli banking system. Pursuant to the previous letter dated August 16, 2022, it emphasized the Banking Supervision Department's expectation that the banks would adopt a high level of sensitivity to new immigrants while maintaining a balance with the need to manage the aforementioned risk. This includes providing access to information in the Russian and Ukrainian languages, as required by Proper Conduct of Banking Business Directive no. 406, on Banking Services for New Immigrants. In addition, the letter made clear that their risk management should not lead to a sweeping refusal to provide services and that in the case of a refusal to transfer funds from Russia or Ukraine to the Israeli banking system or vice versa. The banking corporations must provide a detailed and unambiguous explanation to the customer. The letter also emphasizes that the banking corporations must act in a consistent manner in all of their branches with respect to the documents required to open an account, and they need to define a list of documents required in order to approve the request by a new immigrant to open an account.

Monitoring the banking system's risk management

The Banking Supervision Department carries on an ongoing dialogue with the banking system in which it emphasizes the importance of formulating a risk management policy according to what is stated in the letter from the Supervisor of Banks dated June 8, 2022. This includes close monitoring of activity with Russia. The Banking Supervision Department monitors the banks' management of risk related to the sanctions imposed by the advanced economies and the behavior of the banks toward new immigrants. This includes the gathering of quantitative information on the number of account openings and the transfer of funds by new immigrants arriving from the countries on the sanctions lists and with emphasis on the fact that there are no relevant regulatory barriers and that the banks should facilitate the financial activity of new immigrants.

Information campaigns

The Banking Supervision Department has held meetings with the social organizations that represent the interests of new immigrants from Russia (such as the "The Million Lobby"), with the goal of understanding the difficulties encountered by new immigrants. The meetings are also intended to explain the way in which the Banking Supervision Department assists new immigrants who encounter difficulties in the Israeli banking system, subject to the banks' risk management policy, and to discuss the best ways to assist this population. The Banking Supervision Department held a roundtable discussion with representatives of the banking system, the social organizations, the Ministry of Absorption, and the Jewish Agency, in which possible solutions were discussed for mitigating the problems encountered by new immigrants. In light of the aforementioned, the Bank of Israel will hold an informational meeting for new immigrants, the banking system, the social organizations and entities active in immigration and absorption, which will be accompanied by a digital information campaign translated into Russian on this subject. In addition, a meeting was held with representatives of the Ministry of Absorption to discuss the various problems encountered by new immigrants in the banking system and to come up with ways to provide appropriate solutions.

The activity of the Consumer Enquiries and Inspections Unit

Since the outbreak of the war, the Public Enquiries Unit ("the Unit") within the Banking Supervision Department has dealt with about 100 enquiries and complaints received by the Banking Supervision Department that were referred to the banks, as well as complaints that were received as appeals, in which the Banking Supervision Department decided to become involved.

As a result of the wave of immigration ("Aliyah") to Israel, the methods for submitting an enquiry to the Unit were made more accessible. In addition, information about the Unit's activity and the ways of contacting the ombudsmen at the banks and in the Unit on the Bank of Israel's website also appear in Russian. In addition, the methods of contacting the Unit were expanded, such that it is now also possible to submit an enquiry in Russian. In addition, the Banking Supervision Department provided access to additional information in Russian, including the aforementioned letters from the Supervisor of Banks.

The activity of the interagency taskforce on sanctions

The Banking Supervision Department is part of the interagency taskforce that dealt with the sanctions imposed by the advanced economies on Russia. The taskforce is led by the Foreign Ministry and includes other government ministries and authorities. The relevant activities carried out by the Banking Supervision Department were in coordination with the taskforce.

Box 7.5
The use of machine learning models to monitor and manage the quality of supervisory information

- Many supervisory authorities worldwide, including the Banking Supervision Department in Israel, have during the past decade expanded their use of data as the basis for managing supervisory policy. The growing need to generate insights from data has led to an expanding volume of data that is received and managed on an ongoing basis by the Banking Supervision Department. This has increased the need for specialized automated tools that are highly effective in the management and analysis of big data.

- Machine learning (ML) models make it possible to efficiently deal with the challenges of data management, and in particular, the challenges of examining and ensuring the quality of time series data, including detecting errors in reporting or in the calculation of a series as well as identifying unusual and significant events.

- To ensure the quality of the managed data (known as Data Quality Management—DQM) and detect significant events that are of interest to officials from the various sections of the Banking Supervision Department, the Bank of Israel has developed three ML models: a univariate model for the detection of outlying observations and reporting errors; a multivariate model for the identification of outlying observations in order to detect business outliers; and a model for identifying the approach to a regulatory limit.

- Starting from the end of 2022, the Banking Supervision Department and the Information Technology Department at the Bank of Israel began the development of a large-scale data strategy and in particular a supervisory warning system that includes four types of warnings: status and processes; content and data; trends; and monitoring of risk. The three ML models, which are intended to improve and streamline the work of the Banking Supervision Department, will be included in the supervisory warning system and will address the need for providing warnings with regard to content and data and monitoring of risk.

Part I – The need for smart data management, big data and ML models

Many supervisory authorities worldwide, including the Banking Supervision Department in Israel, have during the past decade expanded their use of data as the basis for managing supervisory policy. In its ongoing work, the Banking Supervision Department analyzes and monitors developments in the areas of stability, competition, innovation, and fairness in the banking system. This process is based on the gathering, management and analysis of current data received from the corporations in the banking system (banks and merchant acquirers).

The growing need to generate insights from data in order for the Banking Supervision Department to fulfill its role has led to an increase in the scope and level of granularity of the data received and managed on an ongoing basis by the Banking Supervision Department (Figure 7.5). The quantity of data received has increased the need to use specialized automated tools for the efficient management and analysis of big data. One of the main challenges in the context of database management at the big data level is related to the quality control of the data and the analysis and accessibility of large amounts of data. While the work of database managers in the past was generally accomplished manually, nowadays the acquisition of knowledge and skill in software and methods that are capable of handling particularly large amounts of data is becoming increasingly critical in their everyday work.

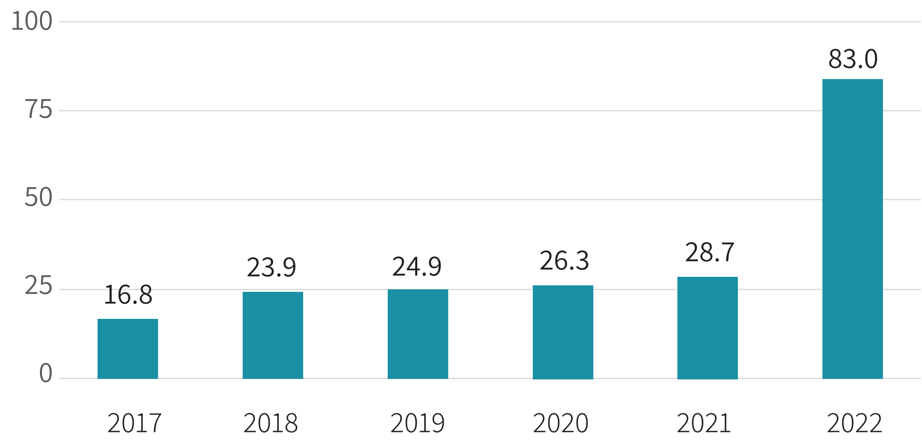
The Bank of Israel's database of time series, which was created in 2021, integrates all of the time series data in the organization.[1] This database includes a wide variety of data series on topics that are generated in the Bank of Israel's various departments. The banking data in the time series database, which are managed by the Banking Supervision Division, include over 240,000 time series that are based on the raw data reported by the supervised entities as well as calculations carried out by the Banking Supervision Department and stored in the time series database. These series are accessible to Banking Supervision Department employees for the ongoing monitoring of the banking system's activity, to researchers and decision makers in the Bank of Israel in order for them to fulfil their functions, and to the public by way of the Bank of Israel website.

The process of managing and analyzing time series includes quality control procedures to identify errors in reporting and calculations and to detect outliers. These procedures constitute a challenge for both database managers and data analysts in the Banking Supervision Department, and given the huge amount of data, it is difficult to overcome these challenges with manual solutions. In many cases, probabilistic models must be utilized to

[1] For further details on the types and volume of reports received by the Banking Supervision Department and input into the time series database, see the box entitled "Management of supervisory information and its value" in the 2021 Annual Survey of Israel's Banking System.

provide effective solutions. ML models enable an automated and efficient response to these challenges. In this box, we present the ML models that were developed at the Bank of Israel for the quality control and monitoring of supervisory data.

Figure 7.5 Data Reported[1] to the Banking Supervision Department, 2017–2022 (million)



1 Number of intact data items, excluding errors in respect of which reporting entities were asked to send an amended report.

SOURCE: Banking Supervision Department.

Part II – A univariate model for the identification of outlying observations in time series data

As part of their ongoing work, database managers must manage the quality of the data (known as Data Quality Management—DQM). The goal of DQM is to ensure a high level of data quality and reliability and thus to allow the data user to generate insights with maximum reliability. The DQM process begins with the precise characterization of the reporting requirements incumbent on the supervised entities. A detailed and precise characterization will prevent errors in reporting and variation in the data across the reporting entities as a result of misunderstandings with regard to the type of information being requested. During the inputting of the information, deterministic tests are carried out for reasonability and logic. For example, a test for the type of data that can be reported in any field—numerical, textual, percentage, etc.; limits on values; and logical checks across fields. After the information is inputted, there are statistical tests to identify outliers in the data. This stage includes ML models that provide a solution to classification problems, where the goal of the model is to classify the new observation as an outlier or normative observation. Statistical learning models make it possible to detect outlying observations that are not apparent from visual inspection and to examine efficiently and rapidly an amount of data that would not be possible using a manual search. At the end of the process, the database manager decides whether to seek clarification of the outlier from the reporting entity, and to request its correction when necessary. This is an important stage in which it is possible to assess the success of the DQM system in identifying reporting problems and the success of the statistical model in categorizing the outliers.

There are two types of outliers that we are interested in highlighting: an error in reporting that needs to be corrected by the reporting entity, and a business outlier, namely an outlying observation that has a business explanation and is not the result of a reporting error, which we would like to detect for purposes of monitoring and risk management.

The univariate model for identifying outliers was developed to detect an outlying observation that is the result of a reporting error. This model examines each series on its own and measures outliers according to the past observations of that series. A good model for identifying outliers should take into account the series' characteristics. Note that these are time series in which the observations are measured sequentially at a given interval, such that there is dependence between an observation and the previous one. For series of this type, there are specialized models that are able to handle their unique characteristics. The series that are being tested have various frequencies (annually, quarterly, monthly, etc.), with the maximum historical depth made possible by the reporting directive. The development of the model takes into account the frequency and the depth of the series, since too small a number of observations make it difficult to understand the behavior of the series based on its history. In such a case, a different model, which does not assume dependency between successive points in time, will be used.

Before using the model, and based on the series' unique characteristics, a pre-processing of the data is sometimes required, with the goal of modifying it to fit the various models. For example, differences for a cumulative series; an estimate of missing observations within the series; calculating the rate of change; etc.

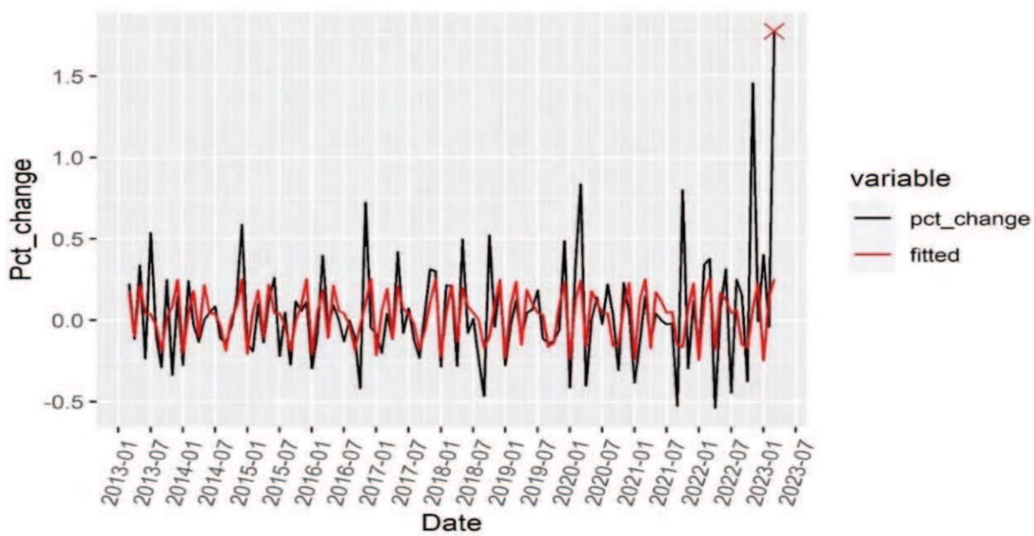
The Seasonal and Trend Decomposition using LOESS (STL) model for series with historical depth

Specialized time series models are usually based on the decomposition of the time series into components, such as trend—which represents the long-term pattern of the series; and seasonality—the short-term behavior of the series, which includes cyclical movements in the series at fixed time intervals. These models learn from the history of these components in order to make a forecast for a future point in time. The STL model estimates the seasonality and the trend of the past observations using the LOESS model (described below). In order to calculate an out-of-sample observation, exponential smoothing (ETS) is used to forecast the next observation based on a weighted average of past observations. This forecast is compared to the actual observation, where the observation is categorized as an outlier according to a statistical threshold rule that is determined outside the model. The calculation of the threshold is based on forecasting error, i.e., the distance between the actual observation and its forecast, relative to the model's forecasting errors for past observation. In order to avoid excessive false warnings, the model's sensitivity to forecasting error is set so that the model will give a warning only in cases of significant outliers.

Figure 7.6 illustrates the implementation of the STL model for a monthly series that is used by the Banking Supervision Department. The black line represents the rates of change calculated on the basis of the original time series data; the red line represents the forecasted rates of change produced by the model and the outlier for March 2023 that was identified by the model (marked by a red X).

The STL model estimates the seasonality and trend components of the series and implements exponential smoothing in order to forecast the next observation, based on a weighted average of the past observations. This forecast is compared to the actual observation, which is classified as an outlier according to a statistical threshold rule that is determined outside the model.

Figure 7.6 Example of Implementation of the STL Model on a Monthly Series Used by the Banking Supervision Department



SOURCE: Based on banks' reports to the Banking Supervision Department.

If the series does not have sufficient historical depth, it is difficult to identify the patterns in the series and to estimate the seasonal and trend components, which is liable to limit the accuracy of the forecasts. In such cases, the LOESS model can be used directly without first decomposing the time series into components, as is done in the STL model. This model is a member of the Locally Weighted Regression family, models that are based on a classic regression but where the observations are weighted so that the observations closer to the forecast observation receive a larger weight. The advantage of weighting the observations is that in the case of insufficient historical depth the forecasting will be based more on the closest observations. The LOESS model supports robustness in that it limits the effect of outlying historical observations on the forecast and thus improves the ability to identify an outlying observation in the next period.

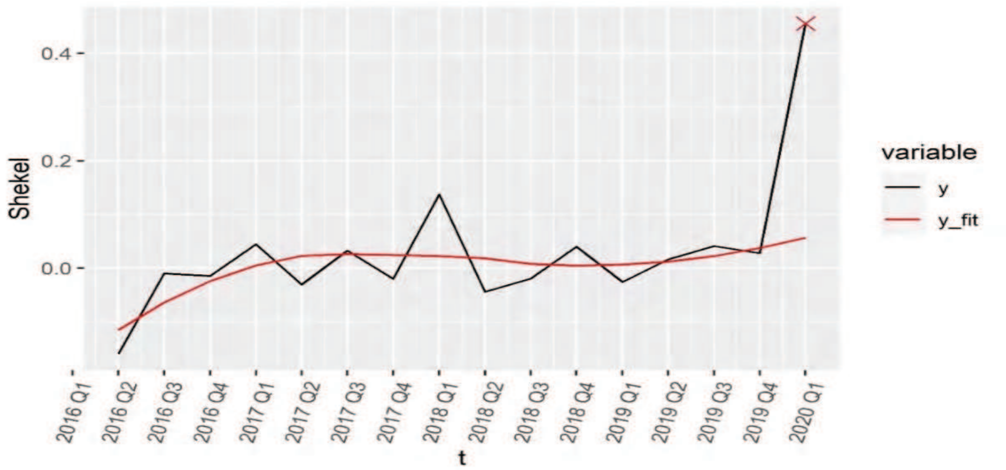
Figure 7.7 illustrates the use of the model for quarterly data that is used by the Banking Supervision Department. The black line represents the rates of change that were calculated on the basis of the original series; the red line represents the rates of change forecasted by the model and in the first quarter of 2020 the outlying observation that was identified by the model (marked by a red X). For the sake of this example, the series was truncated at this date in order to simulate the outlier classification using the existing data for the model in real time.

Part III – A multivariate model for the identification of outliers in time series

A multivariate model for the identification of outliers was developed to detect outliers that result from errors in reporting or business outliers. This model tests a specific observation relative to the past data of the same time series and in relation to other series. The model is appropriate for cases in which a group of series behaves in a similar manner, in some cases influencing each other. The introduction of other series helps the model to learn the expected behavior—from a business perspective—in the next period of the series being investigated, by learning the joint behavior of the series being investigated and the rest of the series. This model provides added value relative to the univariate model in that it learns patterns based on a business connection with other series and takes account of those patterns when forecasting the next period's observation and classifying an observation as an outlier. In order to illustrate the model's mechanism, a simulation is presented below of three series with a high correlation, where series X is the one being investigated (Figure 7.8). The last observation in series X is significantly different from the series' past observations and it would be classified as an outlier in the univariate model. In contrast, if the outliers are estimated while taking into account business similarity between series X and series Y and Z (which are correlated with X), the multivariate model would not classify the last observation as an outlier.

If the series does not have sufficient historical depth to use specialized time series models, it is possible to use the LOESS model, which is based on a classic regression and the weighting of the observations such that the closest ones to the forecasted observation receive larger weights.

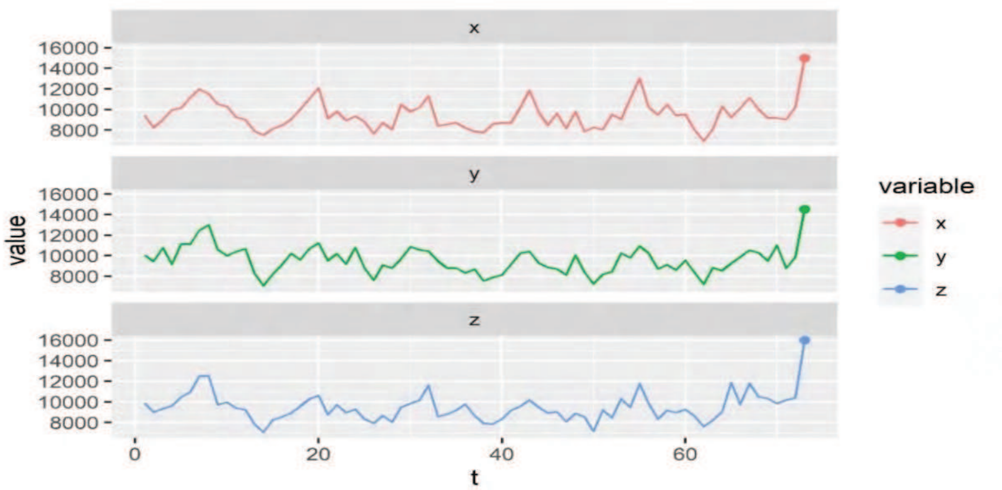
Figure 7.7 Example of Implementation of the LOESS Model on a Quarterly Series Used by the Banking Supervision Department



SOURCE: Based on banks' reports to the Banking Supervision Department.

When the outliers are estimated using the series' past data and when account is also taken of the business similarity between the series being investigated and the series that are correlated with it, the multivariate model will not classify the last observation as an outlier because there was a significant increase observed in all three of the series.

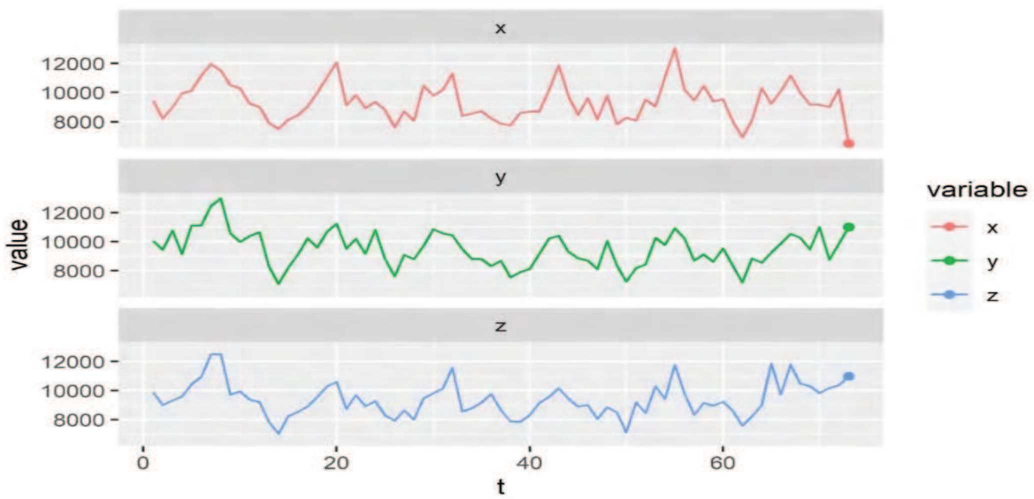
Figure 7.8 Illustration of a Multivariate Model for Identifying Outlier Observations in Three Series with a High Correlation (X,Y,Z)



SOURCE: Banking Supervision Department.

The multivariate model will classify the last observation as an outlier because a significant decline was observed in the series being investigated while there is an increase in the rest of the series during that period.

Figure 7.9 Example of Classification of an Outlier Observation Using a Multivariate Model in Three Series with a High Correlation (X,Y,Z)



SOURCE: Banking Supervision Department.

The multivariate model also provides added value in the opposite case: In Figure 7.9, the last observation in series X is reasonable relative to the past observations in that series and it is not categorized as an outlier by the univariate model. In contrast, when outliers are estimated while taking into account the business similarity between the series being investigated (X) and the services correlated with it (Y and Z), the multivariate model will categorize the last observation as an outlier since a decline was observed in the series being investigated, while an increase was observed in the last observation in the two series correlated with it.

The multivariate model is based on Facebook's Prophet model.[2] In the first stage, the model estimates the series' components, namely trend and seasonality, based on the past values of the series being investigated. In the second stage, the model forecasts the next observation by means of a multivariate regression that includes the components that were estimated, as well as other series that are correlated with the series being investigated. For example, a series of interest rates of various types for various banks: fixed and variable rates of interest with various terms and that apply to credit and deposits. Finally, the Bank of Israel interest rate is added to this group as an additional explanatory variable.

[2] For further information on the model, see Taylor, S.J. and Letham B. (2017). Forecasting at Scale, PeerJ Preprints.

Once the model has created a forecast for the next time period, the gap between the forecasted observation and the actual observation is measured, as in the case of the univariate model. The classification of the observation as an outlier is done by comparing this gap to the rest of the gaps between the model's forecasts for past observations and the actual observations.

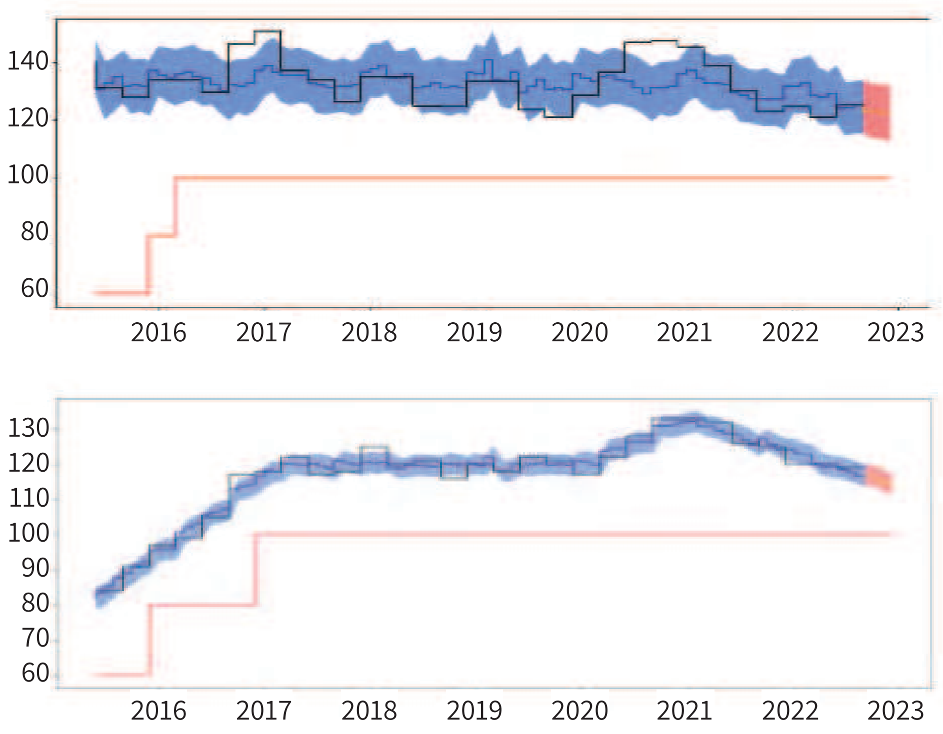
Part IV – The model for identification of "proximity to a regulatory limit"

In order to monitor and manage supervisory risks, a "proximity to a regulatory limit" warning was developed. It provides a warning as a supervised body approaches the limit set by the Banking Supervision Department. The Banking Supervision Department monitors the main indices of supervised bodies and tracks their proximity to supervisory limits that it has determined. For example, the limits for capital adequacy[3] define the minimal level for the ratio of Tier I Capital to risk assets for each supervised entity and the minimum level for the ratio of total capital to weighted risk assets; the limits on industry indebtedness defined for each supervised entity; the maximum level for the ratio of an industry's debt[4] to the public's total debt owed to the banking corporation; and there are a variety of other regulatory limits: the liquidity coverage ratio; the leverage ratio; the net stable funding ratio, etc.

3 See Proper Conduct of Banking Business Directive no. 201.
4 See Proper Conduct of Banking Business Directive no. 315.

In the Prophet model for the identification of "proximity to a regulatory limit", the width of the confidence interval is affected by the volatility of the series. Thus, the model provides a wider confidence interval if the series is more volatile. For a wider confidence interval, the proximity to the limit will be defined more conservatively, such that there will be a warning at a greater distance from the limit.

Figure 7.10-11 Illustration of the Model's Activity on the LCR Limit of 2 Different Banks



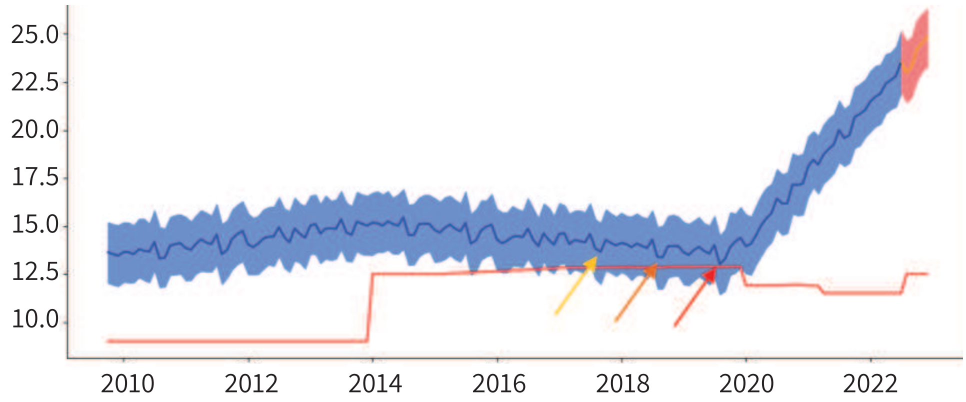
SOURCE: Based on published financial statements.

As an entity that supervises the compliance with these criteria, we must also be aware of instances in which the banking corporations approach the limit and are liable to cross it. To this end, an ML model was developed that relies on the Prophet model and provides a warning as a regulatory limit is approached. The model receives as input the limit for each bank and the actual data for the relevant index. The model is based on a methodology that is tailored to time series, such as the STL model described in Part III above. Each observation of the index is divided into the time series' components, i.e., trend and seasonality. Using these components, the model provides a forecast of the next observation, including a confidence interval around the forecast at a level of precision of 80 percent. The forecast for the next period and its confidence interval help to evaluate proximity to the limit during the current period, given the series' historical behavior.

With the addition of new observations of the index, there is renewed learning of the series' behavior pattern, which can widen or narrow the confidence internal and may influence the sensitivity of the model in providing a warning.

A yellow, orange or red warning relates to the proximity to the regulatory limit with low, intermediate, or high risk, respectively. The thresholds for the warning were determined together with the Banking Supervision Department's experts and the model makes it possible to increase their precision over time.

Figure 7.12 Illustration of the Model's Activity by Various Risk Levels



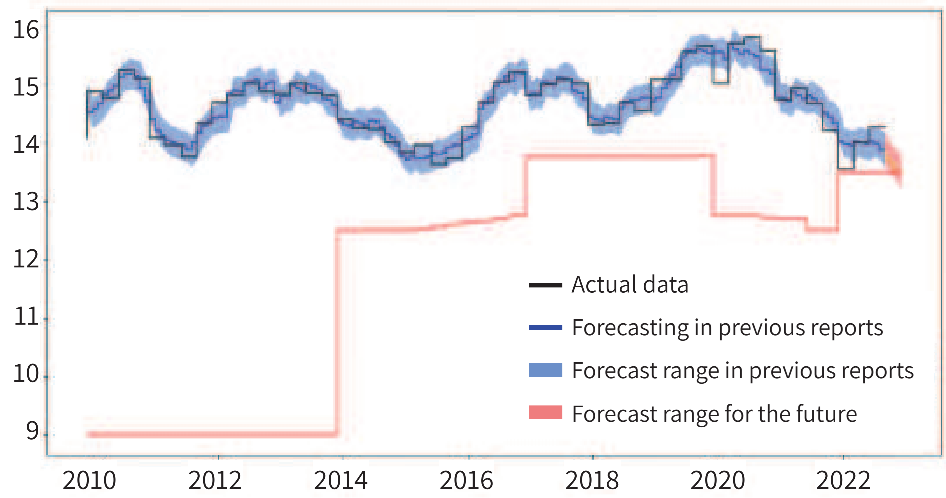
SOURCE: Based on published financial statements.

Figure 7.10 and 7.11 present the limit for the liquidity coverage ratio of two different banks. The red line represents the regulatory limit and the blue line represents the forecasted series, including the forecasting confidence interval, which is represented as a light blue area. The red segment relates to future observations forecasted by the model. It can be seen that in the case of Bank A's ratio, which has a more volatile behavior pattern, the model provides a wider confidence interval relative to Bank B. For a wider confidence interval, the proximity to the limit will be defined more conservatively, such that a warning will be given for a forecast that is farther from the limit.

The mechanism that provides the warnings and categorizes them according to risk level is based on the width of the confidence interval around the forecast of the next observation. Based on the confidence interval, the likelihood that the next observation will reach the limit is calculated. A low warning will not lead to any warning and for higher probabilities there will be a warning with varying severity, where a yellow, orange or red warning relates to convergence at a low, intermediate or high level, respectively. The thresholds for the various warnings were determined together with the relevant experts in the Banking Supervision Department, and the model makes it possible to increase their precision over time.

The chance of a convergence to the regulatory limit in the next period is estimated by means of the confidence interval under the lower threshold for issuing a warning.

Figure 7.13 Implementation of the Model on the Series of Total Capital to Risk Assets Ratio for the Years 2010–2022



SOURCE: Based on published financial statements.

Figure 7.12 illustrates the workings of the model and the division of the warnings according to the various levels of risk. The red line represents the regulatory limit; the blue line represents the forecasted series, including the confidence level represented by the light blue area. The yellow arrow indicates the point at which the model forecasted convergence to the limit with low risk; the orange arrow indicates the point at which it forecasted convergence to the limit with an intermediate risk; and the red arrow indicates the point at which the model forecasted convergence to the limit with high risk.

Figure 7.13 presents the workings of the model in the case of the ratio of total capital to risk assets for the period 2010–22. The red line represents the regulatory limit; the black line represents the actual ratio; and the blue line represents the forecasted series, including the confidence interval for the forecast which is represented by the light blue area. The red segment relates to future observations forecasted by the model. The models expects a continuation of the downward trend in the next period. The chance of significant convergence to the regulatory limit in the next period is estimated by means of the confidence interval under the lower threshold for issuing a warning.

Part V – Assessing the quality of the model

To generate reliable and precise insights from ML models, it is necessary to measure the quality of the model and to make adjustments as follows: The data are divided into a training set and a test set (which includes the observations at the end of the period) where the model learns from the training set, measures the precision of the forecasts using the test set, and makes improvements by calibrating the model's parameters. In order to assess the precision of the model's categorization, the results of the categorization should be monitored over time and verified according to an expert's knowledge in the area. On the completion of the development of the models surveyed above, a ramp-up period will be needed in which their results are evaluated against the expert's knowledge in the area. The verification of the models' results makes it possible to construct a labeled dataset where every observation is tagged as either an outlier or an observation with a normative value (in the model for identifying proximity to a limit, an observation receives a tag of "close the limit" or "not close to the limit"). The labeled set makes it possible to calibrate the models and increase their precision. Events that involve an outlier or convergence to a limit are rare and therefore a longer ramp-up is necessary for the models in order to increase the precision of their parameters, such as thresholds for the detection of outliers.

Part VI – Supervisory warning systems

The three ML models reviewed above are part of the smart supervisory warning system that will help to identify systemic risks when they are developing and to adopt preventative measures. The system, which is being developed by the Banking Supervision Department and the Information Technology Department in the Bank of Israel, will gather various types of information and data from both internal and external sources and will warn of various supervisory events.

The warning system was chosen as one of the steps in the implementation of the data strategy formulation process, with the goal of establishing the Banking Supervision Department as a data-driven supervisory entity, based on the use of advanced technology and analytics. The data strategy formulation process began in 2021 in collaboration with Digital Israel.[5] Emphasis was placed on promoting automation based on AI and ML as part of the application and assimilation of support technologies (SupTech[6]) based on a forward-looking vision.

[5] Currently known as the Israel National Digital Agency.

[6] Supervisory technology – use of specialized technology to streamline and reinforce the supervisory processes from the perspective of the supervisory authorities.

The brainstorming and characterization of the warning system included research into similar systems used by other supervisory entities worldwide as well as interviews and workshops held with the Banking Supervision Department's employees and managers. The system will provide warnings of various kinds: **Content and data** – Warnings related to the data that is reported to the Banking Supervision Department regarding their likelihood and outliers from the perspective of data quality, such as the outlier identification models described above; **Monitoring of risks** – Identification and estimation of immediate and forward-looking risks in the banking system, such as the proximity to a regulatory limit model described above; **Status and processes** – Warnings related to various supervisory processes and their status, such as the reception of a report from a supervised entity, enquiries not dealt with, etc.; **Trends** – Warnings as a result of the identification of trends in the data, such as an increase in credit to a particular industry.

The system will allow for full individualization by defining the destination of each warning and the platform on which it will be sent. There may be variation among the destinations and between the platforms on which a warning will be presented for different risk levels. For example, warnings of different types will be sent to different employees in the Banking Supervision Department; warnings with different risk levels (as in the proximity to a regulatory limit model) will be sent to different groups of workers and will be presented on different platforms.

Following a ramp-up period and an examination of the model included in the warning system, the system will assist in the management of risk, in decision-making and in preserving the stability of the banking system. This will be accomplished by strengthening the ability to deal with the large amounts of data managed by the Banking Supervision Department; improving the efficiency of work processes by reducing manual processing and analysis; monitoring of supervisory events within an optimal time window; and generation of complex insights from the data through the use of AI and ML.

Box 7.6
Customer fraud

- Starting from the end of 2021, there has been a rise in fraud activity committed against customers by criminal scammers disguising themselves as a legitimate company or government entity, in order to trick the victim into giving them sensitive information that will enable them to gain access to the victim's bank accounts. The fraud is aimed at all customers; however, there is a focus on populations with low financial and digital orientation, such as immigrants and the elderly.
- The phenomenon is not unique to Israel and it appears to be an international one, and, according to forecasts, it will continue to grow.
- Despite the growth in this phenomenon, the adverse impact to the banking system does not represent a prudential risk, although there has been some increase in losses to customers.
- Therefore, it is the intention of the Banking Supervision Department to take several measures that will advance the banks' and their customers' readiness and ability to deal with this phenomenon. This involves, among other things, promoting collaboration between governmental entities; promoting the creation of additional protection for customers; awareness campaigns with the goal of increasing the public's awareness; and the clarification of existing relevant regulation.

Starting from the end of 2021 and during the course of 2022, the Banking Supervision Department received reports of incidents of fraud against customers that involves "vishing", using a method of deception that became known as the "Russian sting".[1] Using this method, criminals contact individuals from the FSU by phone, in Russian, while posing as legitimate agents (such as police investigators, representatives of the Bank of Israel or a commercial bank, etc.). They carry out social engineering, sometimes with a high level of sophistication, in which they warn the victims that the bank is about to confiscate their money and that they need to take action as soon as possible, for their own sake and for the sake of others. If the victim does not cooperate, pressure is applied and sometimes even threats. Once the victim is persuaded, he is instructed to carry out various actions, in some instances the physical withdrawal of money from his personal account and its transfer to the criminal, and in others, actions related to his digital account (such as handing over identifying details). After

[1] https://www.gov.il/he/departments/news/police_12-12-22_russian_scam [Hebrew]

the transfer, the criminal cuts off contact. According to information released by the police,[2] it appears that as of the end of 2022, there were hundreds of complaints from all over the country, with the scope of the fraud reaching about NIS 70 million. The information gathered from the banking system indicates that about 2,300 customers have been attacked, with about 37 percent of them losing money.

These events are in addition to the defrauding of various customers that the banking system and its customers are dealing with, such as social engineering, impersonation of the phishing type; smishing (phishing by sms) and vishing (voice phishing) in the cyber space;[3] credit card fraud; check counterfeiting; etc. Customer fraud can be carried out by various criminal scammers and in various ways, with the goal of maximizing their profit or some other benefit.

Customer fraud is not unique to Israel. Various surveys and publications identify it as an international phenomenon, and it is forecast to grow.[4] These occurrences and other indicators have led the Banking Supervision Department to carry out a survey among the banking corporations and credit card companies in order to understand the extent of the phenomenon and its focal points, as a basis for deciding whether there are supervisory actions (and/or other actions) that should be taken. This may involve collaboration with other entities (including national organizations) in order to improve the capabilities for prevention, identification and response and increased awareness of these phenomena.

Based on the information gathered, during 2022 there were various types of customer fraud committed, although the “Russian Sting” was the most prominent. In addition, there was some increase in the scope of the phenomenon, and most of the banking corporations and credit card companies expect the level of risk to rise in 2023. Despite the increase in the scope of the phenomenon, it appears that there was no significant increase in losses to the banking corporations in 2022 relative to 2021 and these losses do not represent a risk to their stability, that of the credit card companies, or that of the banking system as a whole. Nonetheless, it appears that in 2022 there was some increase in the losses to customers as a result of fraud. According to the information gathered, the accumulated losses to customers are estimated to be in the tens of millions of shekels.

The banking corporations and credit card companies are taking various steps to reduce the losses from customer fraud. These include use of security systems to monitor and identify

[2] See footnote 1.

[3] Phishing – social engineering fraud that involves an attempt to obtain personal details from the victim, by means of email. Smishing – phishing carried out by means of sms, as part of the attacker's effort to obtain sensitive information. Vishing – phishing by means of a telephone conversation (voice) in order obtain information from the victim.

[4] Including ENISA Threat Landscape 2022 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, FBI IC3 Internet Crime Report 2022 – https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

these occurrences as early as possible; installation, upgrading and modification of internal control systems; deciding on formal procedures and work processes; management of learning processes, training of workers; and increasing awareness among customers.

In light of the information gathered with respect to the losses to individual customers and based on an understanding of the potential significance of such events, the Banking Supervision Department intends to continue its monitoring of the phenomenon, while verifying that the banking corporations and credit card companies are developing and modifying their monitoring and early detection capabilities.

In addition, and with the goal of increasing public awareness of customer fraud and helping customers to deal with the most common types of fraud, the Financial Education Forum, which is organized by the Banking Supervision Department and which includes the Association of Banks and the banking system, is promoting an information campaign that includes face to face lectures throughout the country; webinars for the public in Hebrew, Arabic, and Russian; the building of a designated website that will include information and videos; and an information campaign in the various media in order to raise public awareness, which is in addition to the steps taken on the national level.

The Banking Supervision Department is working to expand the protection of customers against fraud. In this context, it collaborates with the Ministry of Justice and the Consumer Protection and Fair Trade Authority in order to promote relevant legislation.

Furthermore, the Banking Supervision Department is continuing to promote collaboration with the National Cyber Directorate and the Financial Cyber and Continuity Center in the Ministry of Finance, with the goal of determining to what extent information can be transferred and how to improve the sharing of information on customer fraud among the banking corporations. A further goal is to formulate and promote a program to improve the handling of fraud cases in which there is a need for a rapid response, based on cooperation between various organizations in the space, including the National Cyber Directorate, the police, the Ministry of Communication and others.

Figure 7.14 Types of fraud described in the complaints submitted to the Banking Supervision Department

Impersonating someone else	Impersonating a business or government ministry representative	Impersonating a payment service provider
Bank of Israel, the police, KGB, various NPOs, etc.	The post office, the Customs Authority, the Fines Center of the Enforcement and Collection Authority, the Ministry of Transportation, etc.	A bank or credit card company.
Example: A customer hands over their account details and PIN code received by SMS to someone who has contacted them by mobile phone; someone who impersonates a police officer and even presents a fake police identity. The attacker uses the identifying details to enter the customer's account and withdraw his money.	Example: A customer opens a link sent to him by SMS, which was supposedly from the post office, in order to release a postal item. The customer inputs his credit card number and the secret code that was sent to him by SMS to his cellular phone. The attacker uses the identifying details provided by the customer and debits the customer's credit card in various transactions.	Example: A customer receives a telephone call from someone impersonating a bank security officer who warns him about some event that will soon occur in his account. The attacker asks the customer to provide him with the details of his personal account and the PIN code sent to his mobile phone. The customer provides the requested information and the attacker connects remotely to the customer's account and withdraws his money.

Protection of customers against fraud and exploitation

Given the severity of customer fraud by businesses that do not operate according to consumer protection laws, and in particular against elderly customers, the Banking Supervision Department decided already in 2018 to amend Proper Conduct of Banking Business Directive no. 472 on "Merchant Acquirers and Acquiring Payment Card Transactions". Accordingly, the refusal of an acquirer to provide clearing services or to carry out a particular action for a business against which there is a genuine suspicion[5] of customer fraud, misleading of customers or exploitation will be viewed as a reasonable refusal. This amendment makes it possible for acquirers to close acquiring accounts or to stop an acquiring activity of the aforementioned businesses.

In legal proceedings where an acquirer is sued for not providing acquiring services to businesses based on a genuine concern, the Bank of Israel, together with the Ministry of Justice, provides an opinion in support of the termination of service. The Payment Services Law, 5779–2019, which replaced the Debit Cards Law, 5746–1986, created comprehensive and uniform regulation for various payment services. The law establishes numerous and detailed consumer-related guidelines that are intended to protect customers, increase the public's trust in advanced means of payment and encourage their use.

Section 24 of the Law establishes that a customer will not be responsible for misuse of his means of payment once he has notified his payment service provider accordingly. With regard to the period preceding the notification, the customer will have limited responsibility. This limitation of responsibility will not apply if the customer has submitted the "essential component" to another individual (subject to the exceptions stated in the law). An essential component is defined in the law as a "component of the means of payment that is unique to the payer, including an object or verification detail that was used as part of the means of payment, or a combination of such components, with which the owner of access to the aforementioned component or combination of components can provide a payment instruction…" This could be, for example, a code that the customer received by sms from the issuer of his credit card together with the details of the credit card.

As a result of enquiries received by the Banking Supervision Department regarding instances of phishing, the Bank of Israel consulted with the Ministry of Justice regarding the application of consumer protection established in the Payment Services Law in these circumstances. In response, the Ministry of Justice published an opinion on the question of the application of Section 24 of the Law in the case of impersonating a payment service provider. The opinion made clear that in circumstances in which the customer handed over the essential

[5] The directive provides examples of indicators that lead to a genuine suspicion.

component of his means of payment to a party that was impersonating a payment service provider, the event will be considered "exploitation" and the customer will be eligible for the protection established in the law.[6]

A proposed Protection against Parties Carrying out Violations in Aggravated Circumstances (Amendments to the Legislation) Law, 5783–2023, is currently in the process of approval. It proposes that clarification provided in the opinion regarding Section 24 of the Payment Services Law be made part of the law and in addition, that the law relate to instances of impersonating someone else, such as a security agency, so as to obtain an essential component. This does not include the case in which the payment service provider warns the payer specifically against executing the payment instruction, with the goal of preventing exploitation, and the payer carries it out nonetheless.

It is also proposed that the law will amend the Consumer Protection Law and will expand the powers of the Commissioner of Consumer Protection and Fair Trade, so as to allow him to establish that the perpetrator is a violator in aggravated circumstances, allowing among other things a termination of acquiring.

The public is requested to be alert and to refrain from handing over personal and confidential details and to increase the awareness of the elderly in their environment. We note that the Bank of Israel, the commercial banks and the credit card companies do not contact individuals to request personal and confidential financial details, which includes means of verification and identification that are sent to the individual, such as an sms that includes a personal code.

If you suspect that you have fallen victim to fraud, we recommend that you contact the police, the security department of the banking corporation or the credit card company or the ombudsman as soon as possible. If you do not receive a response or the response is not to your satisfaction, you have the option of submitting a complaint to the Banking Supervision Department.

6 https://www.gov.il/BlobFolder/reports/phishing-opition/he/internternational-law_media_phishing-opition.pdf [Hebrew]

Recommendations and tips in dealing with fraud attempts:

- Do not connect to your bank account from within an SMS or email that you receive.
- Check the address of the website to which you are connecting (verify that it is spelled correctly), particularly when connecting from results of a search on a search engine.
- Provide identifying details only after a return call to the banking corporation's call center to the telephone number that you **yourself found** on the bank's website.
- Do not hand over details of a credit card or PIN code that was sent to you by a link that you received in an SMS or email asking for personal details. **The bank or credit card company will not request the PIN code in a telephone conversation that was not initiated by the customer.**
- If you made a mistake and suspect that you have handed over details to a criminal party, contact the banking corporation immediately and report the incident to them.
- **Periodically check** the activity and transactions in your account in order to identify suspicious activity or inconsistencies.
- **If there is any doubt—there is no doubt** and it is best not to respond to an SMS or telephone conversation or to click on a link before checking with the bank or the company.

Box 7.7
Responsible and fair marketing of consumer loans in the banking system

- Strengthening the organizational culture of fairness in the banking system is one of the main goals of the Banking Supervision Department. To achieve this, the Banking Supervision Department has, among other things, worked to ensure fair conduct in the marketing of consumer credit by the banks and credit card companies. The marketing of credit is an essential and important service; however, if it is carried out inappropriately, it is liable to negatively impact the customer.

- As a direct result, the Banking Supervision Department has taken a number of steps since 2015 to ensure fairness in the marketing of credit, including on-site examination processes. Based on accumulated experience, and in collaboration with the Capital Market, Insurance and Savings Authority, the consumer credit management directive published by the Banking Supervision Department went fully into effect in the end of 2021. Its goal is to provide appropriate protection for consumers of credit.

- The directive establishes principles for consumer protection, including fair marketing conversations, the adjustment of the credit service to the needs of customers and their repayment ability, fair pricing, increased disclosure, and refraining from unnecessarily contacting the customer. Apart from principles for consumer protection, the directive establishes a number of mechanisms and organizational processes intended to increase compliance with the directive. These are anchoring of the duties toward the consumer in policy documents that are approved by the board of directors; strengthening of supervision by the board of directors; creation of marketing scripts that are consistent with consumer protection and monitoring of conversations; an examination of compensation mechanisms; and an obligation to provide instructions to all in the marketing staff.

- The examinations carried out by the Banking Supervision Department revealed that all of the supervised entities have taken steps to significantly improve their work processes in this area and have worked to assimilate and implement the new directive.

- The Banking Supervision Department will continue to monitor and enforce fairness in the marketing of consumer credit using a variety of means available to it. In addition, the alertness of the public, including public and media comment on cases that deviate from the norm, if there are any, and the option of submitting a complaint to the ombudsmen at the supervised entities and if necessary also to the Banking Supervision Department, is one of the most important ways for the Banking Supervision Department to keep abreast of the situation in real time or close to it.

- From a forward-looking perspective, the directive on the management of customer service and support networks, which was published by the Banking Supervision Department in March 2023 and the main sections of which will go into effect in a year, will apply to all types of communication between the supervised entities and their customers, including that which is part of the marketing of credit. According to the directive, the Banking Supervision Department requires the banks "to promote the implementation of a proactive approach, according to which the banking corporations will "place themselves in the customer's "shoes` and will act to create a situation in which the service and support systems will enable a customer to receive relevant information (including information about benefit, risk and cost) in a way that allows the customer to reach a decision that is optimal from the customer's point of view."

Introduction

Strengthening the organizational culture of fairness in the banking system is one of the main goals of the Banking Supervision Department. To accomplish this goal, the Banking Supervision Department has worked, among other things, to ensure fair conduct among the supervised entities in the marketing of consumer credit. Credit marketing is an essential and important service; however, if it carried out inappropriately, it is liable to negatively impact customers. As a direct result, the Banking Supervision Department has adopted a series of measures since 2015 in order to ensure fairness in the marketing of credit, including examinations, following which the supervised entities were required to correct the shortcomings deficiencies that were found.

At the end of 2021, a new directive of the Banking Supervision Department went into effect. Its goal was to protect those who took out consumer loans, and it required the supervised entities to act responsibly and fairly toward customers (Directive no. 311A—Consumer Credit Management; hereinafter "the Directive"). The directive was the result of experience accumulated by the Banking Supervision Department in various examinations that preceded the preparation of the directive. The directive was jointly issued by the Banking Supervision Department and the Capital Market, Insurance and Savings Authority, which supervises non-bank credit providers, with the goal of providing similar consumer protection of customers in the domain of credit.[1]

Following a period in which the marketing of consumer loans slowed due to the COVID-19 pandemic, in 2022 the banks restarted their marketing campaigns by way of advertising and

[1] "We are achieving uniformity in the regulation of consumer credit between the Capital Market Authority and the Banking Supervision Department in the marketing of credit to private consumers by the financial institutions", joint press release, November 25, 2020.

proactively contacting customers using various media.[2] This year, the Banking Supervision Department completed a system-wide examination that was intended to verify the implementation of the directive. A summary of the findings is presented in this box. The examination indicated that there had been major improvements in the marketing process of consumer credit with respect to the welfare of consumers and that the anomalies that had been identified in the past generally did not reappear.

Nonetheless, the Banking Supervision Department directed the banking system's attention to the deficiencies that were found prior to the directive going into effect, in order to verify that the system had improved and that such incidents do not reoccur.

What has changed for customers as a result of the directive and the processes to implement it in the banking system?

The directive established five consumer principles, the purpose of which is to ensure fair behavior on the part of the supervised entities toward customers in the marketing of consumer credit:

- An obligation to carry on a fair marketing conversation.[3]
- An obligation to provide credit service that is appropriate to the customer's needs[4] and is in line with the customer's ability to repay the credit.[5]
- An obligation for fair pricing.[6]
- Obligations of increased disclosure.[7]
- Reducing the frequency of proactive contact and the removal of names from marketing lists.[8]

In parallel to the establishment of these consumer principles, the directive specifies a series of processes and methods to strengthen compliance with them. These include substantial anchoring of the supervised entity's work methods in marketing consumer credit within

---

2 While in 2020, there was a decline in the volume of nonhousing consumer credit in most of the banks, in 2021 there was some recovery and in 2022 an upward trend was observed in the level of marketing efforts.

3 Section 21.2 of Proper Conduct of Banking Business Directive no. 311A. References to the sections below are to this Directive, if otherwise not mentioned.

4 Section 23

5 Section 24–27.

6 Section 16.2.

7 Section 18.

8 Sections 20 and 21.4, respectively.

the policy approved by the board of directors, with the goal of strengthening the board's supervision of senior management; enhanced reporting by senior management to the board of directors on areas related to responsibility and fairness in the providing of credit; a requirement for marketing conversations to be carried out according to scripts that have been checked by a control function that is not business function; a review of the compensation mechanisms to ensure that they do not encourage aggressive marketing that violates the principles; a requirement to document conversations that are not recorded; establishing mechanisms to control compliance with the directive and policy; and a requirement to provide instruction to all of those involved in the marketing of credit.

Implementation of the directive

The survey presented below describes the measures adopted to implement the Directive in the banking system. In order to describe the change, we will present examples of deficiencies that were observed in the past[9] and that were in general dealt with. These are general examples and do not represent any particular supervised entity.

The obligation of fairness in marketing conversations

The directive prohibits "aggressive marketing and putting pressure on customers to make a decision related to a credit transaction."[10] This is in addition to the legal prohibition not to mislead customers; exploit distress, weakness, a lack of experience, or a lack of fluency in the language; or to use unfair influence,[11] in addition to the fiduciary duty and duty of care established in court rulings, which are also anchored in the directive.[12]

The examinations found that the supervised entities have adopted numerous measures to ensure the appropriateness of marketing conversations and that they have worked to change the culture of the dialogue with customers (as described below). This was done by means of checking and modifying the structured scripts that the marketing staff are required to follow; control activities of marketing conversations by the supervised entities' control functions; a check of the compensation mechanism for the credit marketing staff;[13] and internal audit activity in the supervised entities.

[9] Surveys that were carried out by the banks and internal control departments in the supervised entities.

[10] Section 21.2.

[11] Sections 3 and 4 of the Banking (Service to the Customer) Law, 5761–1981.

[12] Section 3.

[13] In the past, deficiencies were discovered in which compensation was based on personal marketing targets that encouraged inappropriate behavior among the marketing staff.

In the past, inappropriate marketing methods that are prohibited by the Banking Supervision Department were sometimes observed including:[14] placing pressure on a customer to make a quick decision – "The loan is only available today, tomorrow it will be canceled"; use of persuasive language; initiating refinancing of cheap loans with a more expensive one; and pressuring a customer by repeated attempts to persuade the customer to accept a loan, sometimes even when the customer has already indicated his lack of interest.

The obligation to align credit service with the needs of the customers and their repayment ability

There is a requirement on the supervised entities to provide credit service in a responsible manner, in order to prevent overleveraging in certain households, particularly disadvantaged ones, and so that customers will be able to repay the credit without substantial hardship. Another requirement is to ensure a fit between the characteristics of the credit being offered to the customer and the purpose of the credit and the needs of the customer.[15] These requirements are a manifestation of the supervisory approach that appropriate disclosure of credit conditions to the customer is not sufficient and that the supervised entity must assist the customer in making an appropriate economic decision.[16]

The directive requires an assessment of the customer's repayment ability, which takes into consideration, among other things, the borrower's overall leverage both at that entity and at other entities as well. This process in general is based on models for assessing the customer's risk, and it is expected of the supervised entities that they will use the credit database maintained by the Bank of Israel and, according to the circumstances, also the open banking mechanism, which was developed jointly with the Banking Supervision Department.

As part of ascertaining the purpose of the loan and to meet the needs of the customer, there is a prohibition on the supervised entities to initiate and market a particular credit service, loan, or credit line without understanding the needs of the customer. In our examination, we found that all the supervised entities had anchored within their policy documents the requirement to adjust credit services to the needs of the customer and the customer's ability to repay the loan without substantial hardship, and that they had chosen a methodology for assessing repayment ability. According to the scripts for the marketing staff, they are to ascertain the needs of the customer and to adjust the credit accordingly. In this area as well, the supervised entities have in place internal control and internal auditing processes.

[14] See the press release by the Banking Supervision Department on December 12, 2018 – Initiated marketing of consumer credit: Examination report findings and Banking Supervision Department requirements.

[15] Sections 2–4 and Section 23. See also "Responsible Lending—From Principle to Implementation", Israel's Banking System, Annual Survey 2018, published on May 22, 2019.

[16] Ibid.

In past examinations, deficiencies were found in the adjusting of credit to the needs of the customer, and the supervised entities were required to resolve them, as mentioned above. This included a lack of effort to ascertain the customer's needs when marketing a particular product as part of a marketing campaign; "suggesting" of needs by the bankers, rather than ascertaining them from the customer (for example, "Many customers intend to go on a holiday, buy a new car or renovate their home; do you also intend to make an atypical expenditure in the near future?"); offering the largest loan possible without properly ascertaining the customer's needs; and even offering a service that is not suited to the customer, following the customer's request for a different service.

The fair pricing obligation

The directive requires the supervised entities to price consumer credit in a fair manner, and in line with the borrower's level of risk and profile. According to the Banking Supervision Department's directives, a customer's level of risk is determined independently by each supervised entity, by means of the model they have developed. This involves a scale of ten rankings, from a customer with the lowest risk to a costumer in financial distress (for example, arrears of 90 days or more on a loan payment). In order to assess a customer's risk, the bank has the right to use not only the criteria specified by the model but also "soft information" on the customer, such as information not yet reflected in quantitative data with respect to an expected decline in his financial situation. The directive requires that there be fair-pricing guidelines in policy documents for consumer credit and on that basis the supervised entities are to formulate and apply a risk-oriented pricing methodology. In general, there must be correlation between the level of risk and the interest rate at the individual customer level and not only at the level of the total credit portfolio.

Increased disclosure obligations

The directive adds disclosure requirements beyond those specified in the Fair Credit Law and the regular rules for proper disclosure that apply to the supervised entities.[17] While the Fair Credit Law and the appropriate disclosure rules focus on the contract stage, in which the customer has already given his consent to the transaction, the directive requires that the supervised entity provide the customer with the substantive details of the credit proposal at the start of the conversation. These include, among other things, the interest rates and the type of interest (such as fixed or variable), the loan period, the size of the monthly payment and the customer's current amount of credit outstanding.

[17] The Fair Credit Law, 5753–1993 and the Banking (Customer Service) (Proper Disclosure and Submitting of Documents) Rules, 5752–1992.

The supervised entity must also inform the customer of his right to cancel the credit transaction within three business days according to the directive and that the explanation he receives must include the ways in which he can do so.

In general, the supervised entity is not meant to propose, as part of the marketing effort, the refinancing of an existing loan at a higher interest rate, including by way of consolidation or enlarging the loans. Such refinancing can take place only as part of a reorganization of a troubled debt (in contrast to proactive marketing based on commercial considerations) or according to a request made by the customer himself, after the implications (namely that the credit will be more costly) have been explained to him.

The supervised entities have anchored the increased disclosure guidelines within the marketing scripts used by the marketing staff and they enforce these guidelines using control and internal audit functions. Improper conversations that are identified by the internal control mechanisms are likely to be taken into consideration in deciding to decrease the compensation of the marketing staff.

The increased disclosure obligations become even more important when a bank initiates a credit to a customer with a significant current account balance or a significant liquid balance in deposits. There is no prohibition to offer credit to deposit owners; however, in these cases there is an obligation to inform the customer of the interest rate on the loan and on the deposit,[18] in order that he can take into account the spread and other important factors (such as the deposit's term or the next exit point, the fine for breaking open the deposit vis-à-vis the interest to be paid on the loan) and therefore make an informed decision.

Reducing the frequency of proactively contacting a customer and the mechanism for removing names from marketing lists

As part of the effort to reduce the frequency of proactively contacting a customer, the supervised entity is prohibited from contacting a customer for a period of no less than three months if he has expressed a lack of interest in obtaining credit. This prohibition is meant to prevent repeated soliciting of customers who have expressed a lack of interest in obtaining credit, which has resulted in dissatisfaction among customers.

In addition, the directive makes is possible for customers to remove themselves from marketing lists, such that the supervised entity will not contact them at all with loan offers. This mechanism is essentially similar to a parallel mechanism established by the Consumer

18 Or in a current account when it has a positive balance, on which interest is not generally paid or is paid but at a very low rate.

Protection Law, according to which the supervised entities are to inform customers of this possibility and to make available to them convenient ways to be removed. Currently, all of the supervised entities make it possible to remove a customer from their marketing lists at the customer's request; however, in practice, it was found that this mechanism is not used much. According to the supervised entities, this is explained by the reduced frequency of solicitation, as mentioned above.

Conclusion

In general, all of the supervised entities have taken a number steps to improve the process of marketing credit to customers and to strengthen its level of fairness.

In its recently completed examination process, the Banking Supervision Department made it clear to the banks, which supplementary measures are to be taken in order to strengthen compliance with the directive with respect to marketing and pricing of consumer credit. Thus, for example, in the area of control there is a particular challenge due the fact that marketing conversations that take place in the branches (as opposed to conversations from the call centers of banks and credit cards companies) are not recorded, which makes it more difficult to achieve the desired level of control. The position of the Banking Supervision Department is that no credit services are to be provided without proper control and therefore all of the supervised entities are required to fine-tune their internal control methods. This can involve the concentration of marketing conversations, or at least most of them, in channels that can be recorded or some other solution, such as physical surveillance in real time, fake clients, customer surveys, etc.

Like any other human activity, mistakes can be made by the personnel of a supervised entity and outsourced service providers, carrying out the marketing conversations in the branches or from the call centers. The Banking Supervision Department will continue to monitor and enforce the requirements of the directive in a variety of ways available to it.[19] At the same time, the alertness of the public, including public and media attention to problematic incidents and the use of the public enquiries mechanism, is one of the important ways to help the Banking Supervision Department understand the situation in real time. Therefore, customers who encounter behavior that is not in line with the principles described above can complain to the ombudsmen in the supervised entities[20] and if they do not get a satisfactory response, they can contact the Banking Supervision Department.[21]

19 See the Banking Supervision Department's Supervision, Correction, and Enforcement Actions Policy.

20 https://www.boi.org.il/information/public-enquiries-unit/complaints-on-banks [Hebrew]

21 https://www.boi.org.il/information/public-enquiries-unit [Hebrew]

With a forward-looking perspective, the directive with respect to customer support and service networks,[22] which was published by the Banking Supervision Department in March 2023 and the main sections of which will go into effect in another year, will apply to all types of communication between the supervised entities and their customers, including the marketing of credit. In the directive, the Banking Supervision Department requires "to promote the implementation of a proactive approach, according to which the banking corporations will 'place themselves in the customer's shoes' and will work to create a situation in which the service and support centers will make it possible for customers to receive relevant information (including information about benefit, risk and cost) in a way that allows them to arrive at a decision that is optimal from their point of view."

22 Proper Conduct of Banking Business Directive 501.