

BANK OF ISRAEL

Office of the Spokesperson and Economic Information

Press release

November 27, 2024

**Remarks by Supervisor of Banks Daniel Hahiashvili at the Banking Supervision Department’s 2024 conference**

The 2024 Banking Supervision Department Conference on Financial Fraud is taking place today. The following are the full remarks by the Supervisor of Banks at the conference:

The past year has been intense and challenging, and has significantly impacted our activities. The Banking Supervision Department, along with the banking system, mobilized to assist reservists and those hurt by the war, reflecting fairness and high social involvement. This is a high standard that the banking system has set for itself, and from here, we can and should only improve.

In the coming year, we will continue to instill a culture of fairness in the banking system, as we have declared in the past, including through regulation—both in terms of the system's commitment to fairness and in more specific areas such as fees and transparency. In the area of competition, our main project is to create a regulatory infrastructure that will allow nonbank entities to enter as competitors in the banking system and raise deposits under a banking license and prudential supervision.

Of course, the main focus will continue to be on stability, and we will continue to promote the Basel 4 guidelines and the implementation of Basel 3 as it relates to capital buffers. At the same time, which also relates to the conference we are holding today, we will guide the banking system in implementing the new directive we issued on managing technology and cyber risks.

The topic of today's conference is financial fraud. We have defined this topic as our supervisory focus, intending to provide supervisory attention and the appropriate resources to address the issue. We have established a dedicated team in the Banking Supervision Department that integrates activities on this topic with the Department's work, from audits on anomaly detection by banks, reviews of fraud and misuse of credit card companies, procedures related to compensating customers in fraud cases, and promoting interministerial cooperation with entities such as the Ministry of Communications, the Police, and the Cyber Directorate to address the issue.

In my remarks, I will talk about the new digital world, the operational risks in such a world, and our duty as a financial system toward customers, with an emphasis on the world of fraud and the regulatory steps we are taking in this context.

Technology, and more so technological innovation, is changing the way people around the world consume services, and this, of course, includes the financial system. For several years now, the rate of direct transactions made by retail customers has been around 90%. When looking by age segment, we see that even the older public are making more direct transactions. It is much more convenient, much simpler, much faster, and from surveys we conduct, it appears that people are also satisfied with this service.

In recent years, the Banking Supervision Department has pushed the banking system toward digital innovation, both for the benefit of the customer and for managing the banking system’s business model risk. One example of such technological advancement is the open banking project led by the Banking Supervision Department. We are still at the beginning of the project, and financial entities have not yet exploited the inherent benefits it offers, but imagine a world where there is a marketplace of financial products, and the customer can choose or receive a product that suits them personally.

There are already over 500,000 active consents in customer accounts. Half a million accounts include permission to access customer information, with tens of millions of API actions passing through this system every month. The presentation of the API world opens up many more possibilities for the banking system and financial entities outside the system, and there are already additional projects on the agenda in this context. One of them is the entire world of payment initiation—essentially having a third party make payments directly from your bank account on existing payment systems, which are also evolving and promoting innovation. Another example is a project we are leading at the Bank of Israel to promote a digital check that will also be based on API. The connection between these worlds will, of course, improve the level of service to customers, the variety of products, and the ability to tailor products to customers fairly.

Technological innovation is, of course, made possible by technologies that are only improving, and I will mention a few from the top:

* The world of automation that allows processes to be carried out efficiently.
* Cloud computing – the ability to use computing resources as needed, find off-the-shelf products tailored to the activity, and enjoy economies of scale.
* Artificial intelligence – AI technology is expected to change the world as we know it. Imagine that the entire world of customer service is carried out by AI—the possibilities in terms of cost improvement, the ability to tailor products to the customer, and more. Even in the world of risk management, AI can bring a significant leap forward. Banks, both globally and in Israel, are beginning to build capabilities in this area, and we are closely monitoring developments. In this regard, an interim report was published by an interministerial team that included the Banking Supervision Department.
* Blockchain technology and the entire world of tokenization – This connects to the future vision of the financial world, at least according to the BIS. If in the past there was a question mark about the role of the banking system, in the current vision, the system will play a central role, but there is no doubt that it will need to continue to upgrade and renew technologically. The BIS published a schema of a future system, based on interconnected financial systems (similar to the Internet), through which individuals and businesses can transfer any financial asset they want, in any amount, at any time, using any device, to any other person, anywhere in the world. Financial transactions will be cheap, secure, and almost immediate. In this regard, we have established a joint team of the Banking Supervision Department and the banking system to examine how tokenization can be promoted in Israel, the characteristics of the business model, and more.
* In the quantum worlds, the issue that particularly concerns us, also in the context of tokenization, is the encryption breaking that quantum computing can provide. We probably have a few more years to prepare for this, but it will come. We are also closely monitoring developments in this area and will issue guidelines to the banking system accordingly.

In the new world, digital risks are significant. Before we touch on fraud, which is one of the significant risks, let's touch on some other risks.

The system is becoming much more complex. It is no longer the bank's on-premises computing system, but many of the systems today are outsourced, and this is even before the expanding transition to cloud applications. In such a world, malfunctions are much more costly and also occur more frequently. We all remember that Friday in July when we woke up to a global CrowdStrike malfunction. In the event, over 8 million computers worldwide were shut down, leading to the halting of flights worldwide, hospital operations, financial systems, and also affecting our financial system, which had to work into the Sabbath to restore its systems.

The Banking Supervision Department is increasing monitoring in this area, mainly to ensure that banking services to customers continue uninterrupted. The public demands 24/7 access to the services they receive from the banking corporations, and the level of availability meets expectations. From the data reported to us, we see availability at the level of 99.9% of the time, certainly a very high level. However, alongside the high availability and complexity of the systems, there are also higher risks, and therefore also malfunctions that have disrupted customer service channels.

Globally, cyber risks are also growing, and in the past year, in view of the war, we have felt it more in the financial system, whether it is an increase in DDoS attacks, data leak incidents, or growing phishing attempts.

Today's conference is about financial fraud. This world of fraud is also only growing, fraud is carried out in various ways and types and sometimes with great sophistication. Many people fall victim to it. We are seeing an increase of tens of percent in financial fraud cases, and in our Department, the number of complaints we receive on the subject is increasing.

Who doesn't know the Nigerian scam? That email or message about the prince from Nigeria who informs us that we are related by blood, and he has no one to bequeath the money to, only us, but to receive the money, we just need to give him our credit card or bank account details. In the case of the Russian scam, they call the customer or contact them in some way, and cause them to go to an ATM or bank branch to withdraw money and transfer it to criminal entities. We have also seen cases where a customer received money into their bank account from a criminal entity without their knowledge, and then the entity, under the pretext of a police representative or bank representative, demanded to receive the money in cash. This contact with the customer ultimately led to direct thefts from the customer's account. Or phishing messages stating that a package from the post office is waiting for us to release it for a few shekels, and in retrospect, it turns out we gave the OTP code to a criminal entity. Additionally, there are vishing scams, which are voice fraud, romantic scams, identity theft, SIM swap, and more. These are frauds that are relatively familiar to us, even before AI technologies that impersonate various entities or perhaps our children or parents...

The financial system has a high responsibility in preventing fraud. As a system through which financial activity is carried out, banks and payment service providers that enable transactions have the ability to identify and prevent fraud already at its inception, whether through verifying and authenticating the identity of the transaction executor, or through anomaly monitoring systems that can identify suspicious patterns in activities at an early stage. Our expectation from the banking system, and in a broader view from the entire financial system—including financial service providers not supervised by us—is to prevent fraud as part of the system's social responsibility toward the public.

This issue also connects to the financial entities’ responsibility to compensate customers who were harmed as a result of fraud. The law defines the division of responsibility between financial entities and customers in this context, with the legislator setting the balance point in favor of the customer, understanding that the financial entity has a better ability to identify and prevent fraud.

Alongside financial corporations, corporations from other industries related to the issue also bear responsibility, specifically communication companies. Additionally, regulators also have a role here. We have the responsibility to create the regulatory and physical infrastructure, to ensure that the financial system and supporting systems, including customers, have the ability to minimize fraud as much as possible. In this context we are emphasizing:

* Financial education – As mentioned, although the tendency in these areas is in favor of customers, the customer also has responsibility, and even if they receive compensation in the end, it is better to avoid this process through early identification and taking security measures from the customer's side as well. We therefore launched campaigns and financial education programs, some with financial entities, to raise public awareness of the issue of fraud.
* Cooperation with other entities – Our responsibility as regulators is to create overall responsibility. An example of this can be seen in the interministerial team established with the Ministry of Communications and the Police, aimed at looking at fraud in a broad and comprehensive manner and examining areas of responsibility and the protection and monitoring capabilities between different industries, such as communication companies through which phishing messages pass, and between different entities. Another example is the activity of an interministerial team to establish a system for financial entities themselves to share information on fraud.
* Regulation and enforcement – Ultimately, our role also requires regulation that is as clear as possible, boundaries, and protections for the customer, but that also advances the market in parallel and conducts enforcement as necessary.