Banking Supervision Department
Technology, Innovation and Cyber Division
Information Technology Regulation and Examination Unit

July 17, 2025
Circular-C-06-2825

Attn: The banking corporations and payment services providers with prudential importance license holders

Re: E-banking
(Proper Conduct of Banking Business Directive No. 367)

Introduction

1. Recently,[1] there has been a significant increase in incidents of customer fraud perpetrated by criminal actors impersonating merchants, government agencies, payment service providers, and other entities, such as the police and various non-profit organizations. This phenomenon is not unique to Israel and appears to be international in scope. Current assessments indicate that it is likely to continue to intensify. While these fraud schemes affect customers broadly, they tend to disproportionately target populations with lower levels of financial and digital literacy, such as immigrants and senior citizens.

2. The fraud incidents confronting the banking system and its customers are diverse and include, among other things, social engineering schemes and fraud methods that exploit the migration of banking services to digital channels. These include phishing, smishing (SMS phishing), and vishing (voice phishing) conducted through online environments, as well as more traditional forms of fraud such as credit card fraud, check forgery, and similar schemes. Fraud against customers and banking corporations may be carried out by various actors and through different methods with the objective of obtaining financial gain or other benefits.

3. The growing prevalence of fraud and the misuse of accounts, including payment accounts, and payment instruments has led the Banking Supervision Department to designate the treatment of financial fraud as a strategic priority for the coming years. As part of this effort, the Department is examining, among other things, the actions required, including regulatory measures, to strengthen capabilities relating to the prevention, detection, response to, and awareness of such fraudulent activities.

4. This current amendment requires a banking corporation to provide another banking corporation with substantiated information in its possession that may assist the recipient banking corporation in identifying and preventing fraud. The collection, use, retention,

[1] Regarding trends in financial fraud, see, among other things, publications by the Banking Supervision Department on "Israel's Banking System"—annual review for 2023 and "Israel's Banking System"—Annual review for 2024.

and transfer of such information shall be carried out in accordance with applicable law, including privacy protection and competition laws.

The obligation to provide such information shall apply to all types of fraud, whether conducted through E-banking services or otherwise, and whether directed against the banking corporation itself or against one of its customers.

This includes fraud perpetrated against the banking corporation by persons other than its employees (including external personnel), fraud committed against a customer of the banking corporation, fraud committed by third parties, and fraud committed by a customer of the banking corporation.

5. The amendment to the Directive is accompanied by the publication of a report pursuant to Section 34 of the Regulatory Principles Law, 5782-2021. The regulation will be subject to an ex post review in accordance with Section 36 of that Law, ten years after its entry into force.

6. Following consultation with the Advisory Committee on Matters Relating to Banking Business and with the approval of the Governor, I have decided to amend Proper Conduct of Banking Business Directive No. 367, "E-banking".

Amendments to the Directive

7. Chapter E – Customer Protection

Section 46A

A banking corporation is required to provide another banking corporation with substantiated information in its possession that may assist the latter in identifying and preventing fraud, including misuse of an account (including a payment account) or misuse of a payment instrument. The use of an account to receive or consolidate funds obtained through fraudulent activity and subsequently transfer them outside the banking corporation is an example of account misuse.

Such information shall be provided as soon as possible, namely, to the extent feasible, shortly after its discovery and after an assessment has been made that it may assist in the identification and prevention of fraud. Information sharing may be carried out through various channels, including bilateral arrangements between banking corporations or through a central entity that will distribute the information to all banking corporations.

The collection, transfer to another banking corporation, retention, and use of such information shall be carried out in accordance with applicable law, including privacy protection laws, and the Economic Competition Law, 5748-1988. The said information transfer shall be carried out regarding all products and services offered by the banking corporation, such as payment services, provision of credit, and regarding all frauds including those that were not carried out in full via e-banking services.

It should be noted that the information provided will be used by the recipient banking corporation as part of the information it is required to consider when making decisions regarding a particular customer or transaction. In order for the recipient banking corporation to be able to rely on the information received, the information shared must be substantiated. Accordingly, information concerning a specific incident shall be shared only after the relevant professional personnel within the originating banking corporation have concluded that there are reasonable grounds to suspect fraud or an attempted fraud.
The extent to which the recipient banking corporation relies on the information received shall be determined at its own discretion and in accordance with its risk management framework.

Section 47

As part of a banking corporation's obligation to monitor developments in fraud methods and threats affecting E-banking services, both in Israel and internationally, and to update, as necessary, the monitoring mechanism required under Section 45 of the Directive, a clarification has been added stating that information received from another banking corporation should also be used for these purposes.

Commencement date
The starting date for the amendments noted in this directive is December 31, 2025.

File update

Following are the update pages for the Proper Conduct of Banking Business Directive file. Following are the directives of the update:

Remove pages	**Insert pages**
(09/21)-[11]-367-1-27	(07/25) [12] 367-1-27

Respectfully,

Daniel Hahiashvili
Supervisor of Banks

July 17, 2025

Regulatory Impact Assessment

Regulation	Proper Conduct of Banking Business Directive No. 367 "E-Banking"
Accompanying Banking Supervision Department circular	2825
Regulation publication date	July 17, 2025
Regulatory function in the Banking Supervision Department	Banking Technology Unit; Technology, Innovation and Cyber Division
Regulation type	Proper Conduct of Banking Business directive
Regulation status	Final
Entry into force	December 31, 2025
Application	The following corporations, as defined in the Banking (Licensing) Law, 5741-1981: (1) a banking corporation; (2) a corporation defined in sections 11(a)(3a) and (3b); (3) a corporation defined in section 11(b); (4) an acquirer as defined in section 36i,
Risk Assessment Report publication date	July 17, 2025

General

Summary of the Regulation

The amendment to Proper Conduct of Banking Business Directive No. 367 "E-Banking" requires banking corporations to relay to a second banking corporation, as soon as possible, established information that may, according to the first banking corporation's assessment, assist the second banking corporation in identifying and preventing fraud, including abuse of an account (including a payment account) or abuse of means of payment. Information collection, transmission, to another bank, retention and use will be performed according to the provisions of law, including privacy laws and the Economic Competition Law, 5748-1988.

Part 1 – The Main Points of the Regulation, Its Aims, Justifications, and Expected Benefits

The Current Situation

Incidents of fraud by criminal entities targeting customers, including the use of bank accounts and means of payment, have increased considerably in recent years. This phenomenon is not exclusive to Israel and is clearly a global phenomenon that is expected to increase, according to forecasts. Such incidents may affect all customers but an analysis of fraud patterns indicates that they are focused on groups that have more limited financial and digital literacy, such as new immigrants and older people.

The banking system performs various actions to address this phenomenon and to significantly reduce the scope of fraud events. Each banking corporation, however, addresses the fraud events that occur in its organization and is unable to make use of the information on similar fraud events that have accumulated in other banking corporations. Moreover, in some cases, fraud events involve multiple banking corporations. A complete picture of the event, based on information from all the banking corporations in the system, could prevent or at least mitigate the scope of the phenomenon and the effects of these incidents on the banking corporations' customers and on the banks themselves.

The Regulation's Expected Benefits

Growth in the number of incidents of fraud and abuse of accounts, including payment accounts, or abuse of means of payment, has motivated the Banking Supervision Department to define the handling of financial fraud as a strategic target focus in forthcoming years. Within this, the Banking Supervision Department also examines the required regulatory steps to increase awareness of these phenomena and improve the ability to prevent, identify, and respond to them.

The banking corporations are not always able to address incidents of fraud independently, especially due to the widespread nature of the phenomenon. Frequently, enforcement agencies become involved at a later stage, after the fraud was completed and the funds were removed from the banking system. Therefore, information sharing at a time as close to possible to the occurrence of the fraud event is the key to the identification, blocking, and even prevention of such incidents in the banking system, in the interests of the banking system's customers and the economy as a whole. The new regulation will require banking corporations to relay to other banking corporations established information that may assist in the identification and prevention of fraud in the other banking corporations, including abuse of accounts (including payment accounts) and abuse of means of payment. In this way, relevant and up-to-date information in the banking system will be brought to the attention of all banking corporations and will allow them to mitigate the damage caused by fraud events, and in some cases will allow them to prevent such incidents altogether. Information sharing is also expected to assist in handling incidents of fraud that simultaneously involve multiple banking corporations.

The Relevant Stakeholders

The amendment to the directive is expected to affect the banking system's customers in general, and especially disadvantaged customer groups, who are the main victims of fraud.

The amendment will assist banking corporations' efforts to address the phenomenon of fraud and mitigate the significant damage that they and their customers consequently sustain. As a result, the amendment is expected to assist efforts to increase customers' trust in the banking system.

The amendment will further increase trust in government institutions, such as the police and the Bank of Israel, and will assist various business organizations to mitigate the damage caused to

them by fraud events in which criminals impersonate these institutions and ostensibly act through them and in their name in order to cause damage to the banking system's customers' assets.

Identifying Similarities and Contradictions in Regulation

1. Privacy laws prohibit, among other things, the transmission of information on a person's private matters, unless the person consents or the transmission is required by law. Accordingly, the regulation determines that collecting, transmitting, retaining, or using information for the purpose of identifying and preventing fraud is subject to the provisions of law, including privacy laws.
2. As the amendment proposes to permit the transmission of information to and from competitors, a consultation was held with the Competition Authority in order to ensure that sharing information among the entities in the banking system does not adversely impact competition, that sharing is limited to information required to address fraud exclusively in the financial system, and that the information is available to all the players who request access to the database, including nonbank entities, under certain conditions. This is similar to the information sharing model related to the need to address cyber events that currently applies to the banking corporation, and on which the Competition Authority issued Public Statement 3/17: Sharing Information in order to Handle Cyber Threats.

To the best of our knowledge, no additional regulation exists that is related to or contradicts the published regulation.

Note that concurrently with the proposed amendment, an approach was made to the Ministry of Justice in order to promote primary legislation that would extend the types of information that banking corporations could share. See additional information in Part 2 below, under "Examined regulatory alternatives and regulatory means."

Part 2 - Main Alternatives and Justification for the Selected Alternative

The main professional issues considered by the regulator

<u>Collaboration between the banking corporations</u>

The main professional issue that was discussed in the course of the regulatory development process was how to create an effective response at the level of the state and the banking system as a whole that would, in the near future and without a significant investment of resources, significantly mitigate the scope of fraud events that cause significant damage to customers and to the banking corporations themselves,

Information sharing between the banking corporations was identified as a means that could considerably assist in mitigating fraud. The banking corporations can use the experiences of other banking corporations that already experienced a similar type of fraud, and in many cases they could perform system-wide fraud identification and measures to prevent fraud events involving multiple banking corporations.

Scope of the information transmitted between the banking corporations

Another issue that emerged is the scope of information to be transmitted between the banking corporations in view of concerns of potential harm to privacy rights and banking confidentiality, and concerns of harm to competition. Accordingly, the regulation includes several elements designed to alleviate these concerns:

- The transmitted information must be established,
- The transmitted information is able, in the opinion of the transferor banking corporation, to assist in the identification and prevention of fraud in the transferee banking corporation,
- The transferee banking corporation may use the transmitted information only for the purpose of identifying and preventing fraud.

Examined regulatory alternatives and regulatory means

The alternative of developing specific and comprehensive primary legislation by the Ministry of Justice to create legal and regulatory certainty, was examined. Such legislation would establish the authority to share information and resolve the concerns about a negative impact on privacy or competition. Such legislation would also regulate the mechanism underlying information sharing beyond the boundaries of the banking system, including information sharing at a later stage with additional financial entities or enforcement agencies.

Examinations indicate that establishing an obligation to share information in primary legislation, as described above, including an option to permit the sharing of sensitive information, would require an extended timeframe due to the complexity of the issue and the average time required to promote legislation, among other factors. All the while, the customers of the banking system would be at risk of significant damage, even to the extent of loss of large amounts of money, harm to their sense of security and trust in the banking system and in state institutions, which increases as this phenomenon spreads and its sophistication grows.

Therefore, the decision was made to implement a rapid solution within the existing regulatory regime of the Banking Supervision Department while concurrently promoting primary legislation. Devising a solution within the framework of Proper Conduct of Banking Business directives makes it possible to define a specific and focused arrangement for the banking system that considers the aspects most relevant to the banking corporations, which frequently serve as the "front-line" of defense against fraud.

Part 3 - The Regulation's Expected Direct and Indirect Effects

Regulation is one of the tools that the Banking Supervision Department uses to improve the abilities to prevent, identify, respond to, and increase awareness of the phenomenon of financial fraud in the banking system. Sharing information between the banking corporations will help each banking corporation to obtain a broad picture of the state of fraud in the banking system and consequently to leverage their ability to address fraud events that involve multiple banking

corporations, and will also help them improve the identification of and response to new fraud events that they had not experienced in the past.

The banks and the credit card companies selected a platform to serve as the infrastructure of the planned information sharing system. The Association of Banks in Israel does not expect the establishment and maintenance of this platform to be complicated and it is not expected to entail significant costs.

A second alternative studied by the banks and the credit card companies was an information sharing platform that uses existing government infrastructure for sharing information to cope with cyber attacks. This alternative was, however, not advanced and therefore a decision was made to implement the alternative described above.

Means and measures of regulatory goal achievement

The number of financial fraud events, their monetary scope, and the number of attempted fraud events (events that failed yet caused indirect damage) can be measured and compared over time. The Banking Supervision Department is also taking action to develop reporting rules for this purpose.

Nonetheless, because regulatory action is only one of the several tools that the Banking Supervision Department uses to increase customers' trust in the banking system with respect to its ability to handle financial fraud and to mitigate the occurrence of such events in the banking corporations, it is difficult to assess the effects and implications of this step in isolation.

Part 4 – Involving the Public and Its Effect on Regulation

1. During the regulation development process, an orderly process of involving the public and all relevant stakeholders took place, in accordance with the Regulation Principles Law. 5782-2021 and the procedures of the Banking Supervision Department.
2. The first draft was sent to the members of the Advisory Committee on Banking Business Affairs on January 6, 2025. The members of the committee are, by law, representatives of the banking system, representatives of the public, and representatives of other financial regulators. The deadline for receiving comments was January 13, 2025, in accordance with the Banking Ordinance, 1941.
3. A draft for consultation with the public before publication of the final regulation was distributed on April 1, 2025, and the deadline for submitting comments was set at April 20, 2025.
4. In the public consultation, several requests for clarification were received, including clarifications regarding the need to define arrangements for the limits of liability for the use of and actions based on information received from another member of the information sharing system; clarifications regarding the definition of established information, which is a condition

of information sharing according to the directive; and clarifications regarding the operational neutrality of the required information sharing solution. Appropriate clarifications were incorporated in the explanatory note to the directive.

Also received were requests to extend the date of the directive's entry into force to six months from its publication date, in lieu of three months from its publication date. The reasoning behind the request was based mainly on the time required to complete the technological implementation of the selected solution, and the need to regulate the legal aspects, including the required consent of the various entities expected to use the solution. These requests were accepted.

Part 5 - Other

Retrospective assessment

The Banking Supervision Department reviews the need to revise the supervisory policy or additional or complementary regulatory actions with respect to the phenomenon of fraud in the banking system, as part of its ongoing operations, where such reviews include monitoring the number of fraud events, their scope, and the methods to prevent them commonly used around the world. The Banking Supervision Department will revise the directive insofar as a need to do so emerges or primary legislation requires. The regulation will be retrospectively examined, in accordance with the requirements of the Regulation Principles Law, 5782-2021, no later than at the conclusion of the 10-year period from the date of its entry into force.