State Comptroller's Report – Cyber and Information Systems | May 2023

The Ministry of Justice – Enforcement and Collection Authority

Privacy Protection and Information Security in the Center for Collection of Fines, Fees and Expenses Systems in the Enforcement and Collection Authority

Privacy Protection and Information Security in the Center for Collection of Fines, Fees and Expenses Systems in the Enforcement and Collection Authority

Background

The Center for the Collection of Fines, Fees, and Expenses in the Enforcement and Collection Authority (the Center for Collection of Fines or the Center) collects debts for the State Treasury and public bodies and compensation awarded to victims of crime in criminal proceedings. As of February 2023, the debt balance in the open cases at the Center for Collection of Fines was about NIS 6.8 billion. The Center was granted collection powers to collect debts, including demanding information about the debtor from a public body. To effectively collect debts, the Center work is managed through a computerized system containing a large-scale database of about 3 million debtors, including, among other things, names, identity numbers, residential addresses, telephone numbers, details of debtors' assets, information from the National Insurance Institute, from the Licensing Division of the Ministry of Transport and other authorities.

As far as the privacy protection and information security is concerned, the Center for Collection of Fines is required to comply with the provisions of the law, including the Privacy Protection Law, 1981, and the regulations promulgated thereunder, government resolutions and the procedures and guidelines of the bodies that regulate the issue, including the Unit for Cyber Protection in the Government, which is a professional guiding body in cyber protection.

Key Figures

3 million

the number of debtors included in the Center for Collection of Fines' databases

about NIS 6.8 billion

the total debt balance in the open cases in the Center for Collection of Fines

only 7%

the rate of unusual events[1] (99 out of 1,391) in September 2022 examined by the Center's control factors

52%

the access permission rate (23 out of 44) to the Center's operational system given without requesting the approval of the access permission Administrator at the Enforcement and Collection Authority

14 access permission

of employees of the information call center to the Center's database were not revoked despite the termination of their employment, within one to 13 months before the audit date

21%

the information call center employees rate (20 out of 94) who used the system without a smart card associated with them

Audit Actions

From September 2021 to October 2022, the State Comptroller's Office audited aspects of Privacy Protection and information security in the Center for Collection of Fines systems. The audit examined the access documentation, the use of the information systems and the changes therein, the set of access permissions to the information systems in the Center, and contending with penetration risk into the information systems. Completion examinations were carried out in January and February 2023.

The audit was conducted at the Center for the Collection of Fines, Fees, and Expenses at the Enforcement and Collection Authority and the Authority's headquarters. Completion examinations were conducted at the Privacy Protection Authority at the Ministry of Justice and the Unit for Cyber Protection in the Government (Yahav) at the National Digital Agency.

1 Business events defined as unusual events in the operational system of the Center for Collection of Fines and warrant individual examination whether they were justified, such as closing a debt above a certain sum without payment.

At the same time, the State Comptroller's Office examined further activities of the Center, such as: managing the debt collection process from the stage of entering the case, sending payment demands, and performing various collection procedures; The debt rescheduling mechanisms, reductions and addition of arrears and the cancellation of debts; The management of the debt collection process of compensation for crime victims and the Communication with the crime victims. These audit findings were published in the State Comptroller's report from May 2023[2].

The Knesset State Audit Committee sub-committee decided not to bring this report in its entirety before the Knesset but to publish only parts thereof, to protect the state's security under Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].

Key Findings

- **Documentation of the Access to Information Center's Systems and Control Over it –** the Center for Collection of Fines does not document the users access to its system, to the extensive and sensitive information it holds and does not control it. Thus, in the event of user anomalies, it is impossible to detect them and stop them.
- **Examination of Unusual Events in the System –** although in 2016, the Center defined a list of 13 unusual events that require individual examination if justified, in September 2022, 1,391 unusual events were recorded, of which only 99 (7%) were examined. In addition, since 2016, the Center did not update the list of unusual events in the system.
- **Management of Access Permissions to the Center's System –** out of 44 user access permissions given in the dedicated computerized system (system B) in 2021, 23 (52%) of them were given without requesting the approval of the access Permission Administrator, as required by the Center's procedure.
- **Control of the Active access Permissions in the Center's Operational System and their Scope –** starting in July 2020, the beginning of the Center's using System B, and until the audit completion in October 2022, no control was performed on the access permissions to the system, nor the requirement to revoke permissions (due to inconsistency with the nature of the position or due to a change of position).
- **The Access Permissions Scope to the Center's operational system –** all the Center's employees, and the information call center employees who are outsourced, have

2 State Comptroller, **State Comptroller's Annual Audit Report, May 2023**, "The Center for the Collection of Fines at the Enforcement and Collection Authority", p. 1723.

access to the complete information in the operational system, containing about millions of debtors, without examining whether the scope of access to the information is necessary according to their position description.

- **The Access Permissions Management of the Information Call Center Employees –** the access permissions of 14 former call center employees to the Center's operational system were not revoked despite the termination of their employment within one to 13 months before the audit date. Furthermore, the Center did not block the smart cards of employees who no longer work there, and in practice, in different cases, the call center employees uses the cards and passwords of these employees.

- **Management of Permissions Access to System C –** access permissions to System C, generating cross-sectional reports on the Center's activities and detailed information on individual cases, were given to employees whose position nature does not require access to the information in the system. About 40% of the holders of permissions to System C (20 out of 52) did not use System C, at least since 2021.

- **The Enforcement and Collection Authority's Contending with the Penetration Risk into the Center Operational System –** in a penetration test carried out by Yahav, deficiencies were found at the infrastructure level that could pose a significant risk if a penetration into the organization's network occurred. The audit raised that despite the above findings, the Enforcement and Collection Authority did not implement a specific dedicated technological security solution in its systems, including in the Center's operational system.

Key Recommendations

- The Center for Collection of Fines should establish a system to document the users access to the information in the operational system and periodiclly control the access under the provisions of the Information Security Regulations and the ISO 27001 standard (which is an international standard that addresses the establishment of a system for managing organizational information security and the ongoing process of system management and improvement).

- The Center should carry out quality and regular control over unusual events. It is also recommended to consider improving the list of unusual events in the system.

- The access permission Coordinator should avoid applying access permissions without the access permission Administrator's approval.

- The Enforcement and Collection Authority should examine the scope of the access permissions to the Center's operational system of employees in the various positions and

periodically control them under Yahav's directives and the Enforcement and Collection Authority procedures.

- It is appropriate that the Center consider limiting the access possibilities of the information call center employees to the information in its operational system based on the inquiries received at the center. In addition, it should periodically control the access permissions of the call center employees and refrain from using the system access permissions of employees who are not employed at the call center or from transferring smart cards from one employee to another.

- It is recommended that the Enforcement and Collection Authority individually examine the access permissions granted to System C according to the need and relevance to the permission holder position, thus reducing the access permission holders scope to the minimum necessary.

- The Enforcement and Collection Authority should promote the tendering process and implement a specific dedicated technological security solution, ensuring maximum protection of the information assets of the Enforcement and Collection Authority under Yahav's directives.

The Procedure for Granting Access Permissions in Practice for the Center's Operational System

According to the Center for Collection of Fines' data, processed by the State Comptroller's Office.

Summary

This report presents deficiencies in the privacy protection and information security in the information systems of the Center for Collection of Fines of the Enforcement and Collection Authority, including the lack of documentation of users' access to the information in the Center's operational system and consequently, the lack of control over that access; Failure to perform adequate monitoring of unusual events in the system; Poor management of the process of granting access permissions to the Center's operational system and of their supervision and control; Unlimited scope of access of the system users to its information; Inadequate management of the information call center employees' access permissions to the system; As well as the risk of external attackers penetrating the Center for Collection of Fines' systems.

These deficiencies are not in line with the provisions of the law, including the Provacy Protection Law and the regulations promulgated thereunder, the relevant government resolutions, and the guidelines of the bodies regulating the matter. This is reinforced given that the Center's operational system is classified as a database requiring a high level of security by the provisions of the Information Security Regulations,.

The Enforcement and Collection Authority and the Center should quickly follow the instructions of the relevant bodies to prevent the leaking of information from the organization and maintain its integrity. In addition, they should establish a system for documentation and control regarding using the Center's information systems. Furthermore, they should periodically control the access permissions of the Center's employees and even examine the access scope of the permissions to the Center's operational system by employees in various positions. Moreover, they should control the access permissions of the call center employees, and it is appropriate that the Center consider limiting the access of the call center employees to its operational system. Additionally, the Enforcement and Collection Authority should promote the tendering process and implement a specific dedicated technological security solution in its systems, ensuring maximum protection of its information assets.

The Center's extensive database includes sensitive information of about 3 million debtors. The debt sums handled by the Center as of the audit completion was about NIS 6.8 billion. Hence, the need to maintain the information systems to prevent damage to the integrity of the information and functional continuity of the Center for Collection of Fines in providing services, and to prevent the leaking of information from the database or to prevent their disclosure to unauthorized parties.