NEW YORK CITY HOUSING DEVELOPMENT CORPORATION

MEMORANDUM

To: Audit Committee

From: Mary Hom
Chief Risk Officer

Date: May 28, 2024

Re: Internal Audit Report

Since the last report to the Audit Committee on March 27, 2024, one internal audit was completed. A copy of the report is attached, and a summary is as follows:

2023 Bank Token Management (assurance)

Objective(s):
The objectives of this audit were to:

- To determine if user access to banks that require tokens is appropriate and up-to-date;
- To determine if administration of tokens (which includes provisioning, removing/updating, and distributing of physical/virtual tokens) is performed in accordance with best practices; and
- To determine if policies, procedures, and proper training is provided to employees that administer tokens, and users who are authorized to perform token required activities.

Audit Results:
Upon completion of the audit, we noted no matters involving internal controls that we considered material weaknesses. Opportunities exist to further enhance controls for Bank Token Management to ensure completeness and accuracy of token users and inventory, and authorization of new users. This would include the development of a token authorization form and token inventory. Management has commenced development of a semi-annual review process of user access to banks.

Objectives:

- To determine if user access to banks that require tokens is appropriate and up-to-date;
- To determine if administration of tokens which includes provisioning, removing/updating, and distributing of physical/ virtual tokens is performed in accordance with best practices; and
- To determine if policies, procedures, and proper training is provided to employees that administer tokens and users who are authorized to perform token required activities.

Scope:

The audit period covered activity from January 1, 2023 through October 31, 2023.

Background:

With the escalating threat of social engineering tactics, particularly phishing simulations aimed at instructing individuals to execute fraudulent wire transfers, financial institutions have enhanced their focus on implementing robust safeguards and controls to anticipate breaches. Among these measures, bank tokens and the expanded utilization of multi-factor authentication (MFA) stand out as effective defense mechanisms. Bank tokens are devices that help authenticate digital bank users. MFA involves the combination of knowledge-based factors, like passwords or PIN numbers, with possession-based factors, such as physical or virtual tokens, thereby increasing the security against cyber threats.

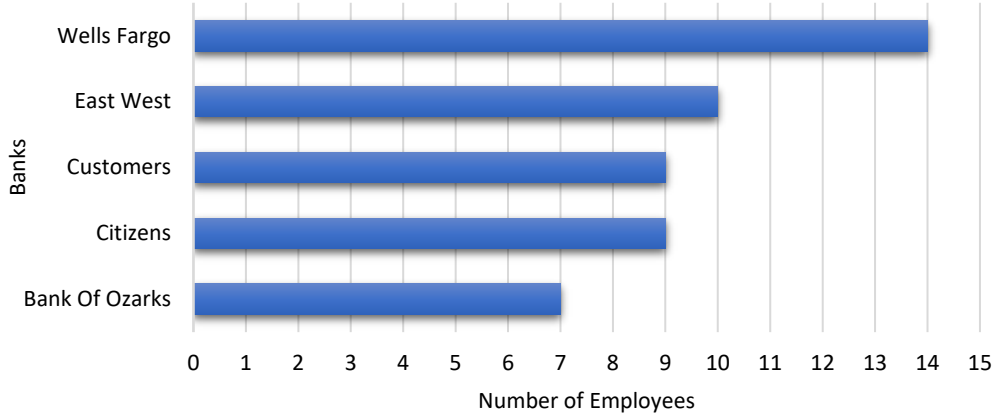
The importance of authenticating a user is critical when performing high risk activities such as executing wire transfers. As a result, HDC, in collaboration with the banks facilitating these transactions, has instituted MFA protocols, leveraging a user's personal password in conjunction with a one-time password generated through either a physical token device or a virtual token.

To oversee the management of tokens, administrators have been designated within the IT and Credit Risk departments of HDC. Presently, three administrators are assigned with overseeing token management across five partner banks. Their main roles and responsibilities include ordering tokens from banks, setting up users and role assignment, and releasing locks or resetting passwords. However, it's important to note that administrators lack the authority to authorize new user access. This responsibility lies with the Managing Director of Cash Management, who is required to notify the token administrators via email whenever a new user needs to be provisioned access for a specific bank.

Results:

Upon completion of the audit, we noted no matters involving internal controls that we considered material weaknesses. Opportunities exist to further enhance controls for Bank Token Management to ensure completeness and accuracy of token users and inventory, and authorization of new users. This would include the development of a token authorization form and token inventory. Additionally, to ensure effective governance and oversight of tokens, management should continue to develop a semi-annual review process of user access to banks.

HDC Employee Access To Banks



*There are a total of 15 HDC employees overall that have access to banks (IT - 2, Credit Risk - 1, Cash Management - 7, and Loan Servicing - 5).

Internal Controls

- ✓ Robust log-in process to banks (including MFA)
- ✓ Segregation of duties
- ✓ Dual approval to obtain tokens
- ✓ Documented policies and procedures
- ✓ Tokens are safeguarded in a secure environment