State of New York

Barry L. Kluger
Inspector General

Office of the Inspector General
Metropolitan Transportation Authority
Two Penn Plaza, 5th Floor
New York, New York 10121
212-878-0000

February 6, 2019

Mr. Andy Byford
President
MTA New York City Transit
2 Broadway, 20th Floor
New York, NY 10004

Re: Unauthorized Use of Non-Employee Access Passes
MTA/OIG #2018-52

Dear Mr. Byford:

MTA New York City Transit (NYC Transit) conducts business with numerous contractors, consultants, concessionaires, and others (collectively vendors), who need access to transit-system property during the course of their business dealings with the agency. To provide such access, NYC Transit issues non-employee access passes to these vendors for business-use only.

The Office of the MTA Inspector General (OIG), as part of our ongoing efforts to ensure system security, reviewed the vendors' use of these passes to determine if such usage was in accordance with the stated business purposes and effectively monitored by the agency to prevent unauthorized use. As described more fully below, our review identified several passholders who clearly misused their pass privileges through non-business use, as a result of which NYC Transit deactivated their passes and obtained reimbursement from the offending vendor, as appropriate. Going forward, we recommend enhanced monitoring of the passes to more effectively detect and deter unauthorized use. In your response to our preliminary report, dated December 28, 2018 and more fully described below, you accepted our five recommendations, noting that the agency has fully implemented two of them and is moving toward implementation of the remaining three.

BACKGROUND

NYC Transit's Non-Employee Access Passes Policy (Policy) defines six non-employee access pass types. The two types that are the subject of this review are the System Access (SA) and MetroCard Temporary Transportation (MTT) passes[1]. Both of these passes can currently be

[1] The other four non-employee pass types are: Building Access and Visitor passes, which do not allow the holders to independently gain entry into the subway system or buses; and School Intern and Mobility Instructor passes, which provide the holders access to the subway system and buses on weekdays between 5:30 AM and 8:00 PM only. As used in this report, references to "non-employee access passes" mean only the SA and MTT passes.

used to access NYC Transit facilities. Additionally, while both cards have the *capability* to provide subway and bus access to passholders by swiping at the turnstiles and fareboxes respectively, *the Policy* does not authorize the use of the SA pass to gain entry to buses. Further, the Policy restricts these passes to MTA-related-business use, and expressly prohibits them from being used for commutation to and from the passholder's residence and work location. The NYC Transit Department of Security (Security) is responsible for issuing, maintaining accurate records regarding, and monitoring the usage of these non-employee access passes.

To obtain a pass, the Policy requires that each applicant fill out a Non-employee Access Pass Application specifying their duties/tasks to be performed, work days and hours, work locations, and the start/end dates. As part of the application process, the applicant must accept and abide by the conditions of use, specifically that the non-employee access pass is not to be used for commutation; the pass is to be used only to access the portion of the NYC Transit system or property relating to specific duties; and the pass is only to be used during the hours when performing work. In addition, the Policy requires that the applicant's employer provide an affidavit attesting that all of the passes are needed for the performance of its work for the MTA. In signing the affidavit, the employer makes a sworn representation that "*every effort will be made by our company to avoid or eliminate any unauthorized use of the passes issued pursuant to this request and that all passes issued to our personnel will be strictly limited to carrying out the duties required and necessary in connection with our contract with MTA New York City Transit.*"

FINDINGS

Improper Use of Passes

NYC Transit records show that 700 SA and 540 MTT passes were active in 2017. Of these, our review targeted those with the highest number of swipes at the subway turnstiles and bus fareboxes, resulting in our in-depth analysis of five SA and 19 MTT passes. To determine whether these passes were improperly used, we isolated usage patterns that were not consistent with the passholders' duties, work locations, and work hours as stated in their pass applications. As a result, we found that four of the 24 passholders used their Non-Employee Access Passes for unauthorized purposes:

- Two employees of a vendor that provides advertisement display services in NYC Transit subway and bus systems, routinely used their MTT passes for commuting on weekdays or during weekends when not scheduled to work. Employees were granted these passes only to post and maintain advertisement displays throughout the subway system and buses. We found that these two employees, who worked Monday through Friday during the hours from 6:00 AM to 3:30 PM, swiped a total of 1,018 times on weekends and at other times outside their scheduled work hours.

We shared this information with the project manager for NYC Transit Marketing & Service Information Department, who reviewed the pass usage in question with the vendor. The vendor confirmed that the usage was unauthorized and agreed to reimburse NYC Transit for the unauthorized use of the passes. The project manager also informed the OIG that the vendor has reinstructed its employees that their MTT passes are to be used only for conducting contractual work. Furthermore, in accordance with the Policy, Security has since deactivated these two passes without issuing replacements.

- One employee of a New York City agency repeatedly misused his System Access pass, which had been issued to the agency for employees to service the BioWatch Program[2] equipment located in the subway system. Eighty-five percent of the card swipes for this employee were for buses along a particular route, which was consistent with a commuting pattern. Aside from any commuting, which is flatly prohibited, this usage violated the Policy both because the System Access pass is only authorized to access the part of the subway system where the BioWatch Program equipment is located and because the SA pass is not authorized for use on buses. Additionally, we learned that agency employees are issued city-owned cars to travel to subway locations where the equipment is deployed.

  We estimated that this employee's improper usage resulted in lost revenue of more than $2,500 to NYC Transit. Security confirmed our determination and this pass had since expired. The employee's behavior was referred to New York City Department of Investigation (DOI) for further review.

- One employee of a vendor that provided inter-office mail delivery and other building services, had two MTT passes that were active and being used during the same eight-month period from May to December 2017. MTT passes allow vendor employees to make their inter-office mail runs to and from various MTA agency locations using the subway or buses. In this case, the employee was issued one pass, lost it, and reported the loss to Security as required in May 2017. Security issued a replacement shortly thereafter but neglected to submit a request to MetroCard Operations to deactivate the lost pass. As a result, that pass remained usable and was swiped 1,130 times during the eight months following the loss by an unknown party for unauthorized travel.

  Upon learning from us that the reported lost pass was never deactivated, the Security manager responsible for the monitoring of non-employee access passes acknowledged the mistake and deactivated the pass. Our review of other reported lost passes indicated that this neglected deactivation appears to be an isolated incident.

---

[2] BioWatch is a U.S. Department of Homeland Security's program established in 2003 to provide air-monitoring, analysis, notification procedures, and risk assessment to minimize the catastrophic impact of a biological attack (https://www.dhs.gov/biowatch-program).

As described above, both SA and MTT passes are accepted by subway turnstiles and bus fareboxes although the Policy does not authorize the use of SA passes on a bus. Regarding the employees who used his SA pass on a bus, misuse of that pass was evident from the usage itself. However, misuse of the MTT passes by two other employees on a bus was not readily apparent, and required some analysis to determine if each use was for a business purpose. Given this technology/Policy inconsistency, coupled with the reality that few if any SA/MTT passholders need access to buses for MTA business, we believe that allowing these passes to work in bus fare machines creates a vulnerability for the agency. Significantly, in discussions with Security, OIG staff learned that improper use of these passes would be minimized, if not eliminated, by electronically programming them to work only at subway turnstiles unless bus access has been specifically approved by the agency. Indeed, as a result of our review, Security has already taken action to prevent the use of SA passes on buses.

Inadequate Oversight of Passes

The Policy dictates that each department is responsible for conducting periodic audits of pass use to ensure that applicants are complying with applicable conditions and requirements. However, we found that the project managers rarely conducted such reviews even with periodic reminders from Security to do so. In our discussions with these project managers, we were often told that the department did not have sufficient personnel resources to conduct reviews. Because of this lack of monitoring, improper use of non-employee access passes can go undetected and undeterred at the department level.

For its part, Security did randomly review selected non-employee access passes for improper usage. While such review was time-consuming, Security staff had some success. For example, Security discovered extensive unauthorized use of 35 of the 39 SA passes issued to a vendor that operates a marketplace of retail shops and food sellers in an underground corridor leading to the 59th Street - Columbus Circle subway station entrance. These passes were issued to the vendor for the sole purpose of allowing the marketplace employees access to the bathrooms located inside of the 59th Street subway station. However, Security, together with the contractor, identified approximately 4,000 unauthorized swipes at subway stations throughout the system, as well as on buses during the one-year period from January 2017 - 2018. This determination resulted in the vendor reimbursing NYC Transit $11,000 for the unauthorized use. Security also deactivated the 35 SA passes involved.

While this review clearly evidenced Security's diligence in monitoring pass usage, it also illustrated the inefficiency of its review process, which required staff to manually sift through pages of a printed reports to identify unauthorized transactions—a process that is simply too labor intensive to be effectively performed on a regular basis. Contributing to this problem was that NYC Transit's MetroCard fare collection system is operated on an antiquated computer system with limited processing capacity. As a result, MetroCard Operations cannot extract large amounts of usage data at one time without negatively affecting the system performance.

Depending on the daily system processing demand, usage data for only a handful of passes can be extracted each day and data can only be provided in limited file formats[3] that cannot be electronically analyzed. These data management problems have hampered the monitoring ability of the Security staff, and will likely also hamper monitoring efforts by the user departments going forward.

On a positive note, in conducting our review we developed an approach whereby a large amount of pass-usage data could be efficiently analyzed electronically, which allowed us to identify potentially-abusive usage patterns for more detailed analysis. In our view, Security staff and user departments' project managers could increase their effectiveness and efficiency in monitoring pass usage by adopting our process of converting the usage data from an unstructured text format to a tabular format, such as a Microsoft Excel worksheet. This file conversion allowed us to quickly analyze the usage data for a large number of passes as opposed to manually reviewing the usage of just a few random passes at a time. To provide further assistance, we shared our methodology with Security staff. Security was receptive to our suggestion and indicated that they would use it to improve their analysis of pass usage.

And lastly, NYC Transit must simply do more to help employers comply with the obligations they assumed when obtaining access passes for their employees. As noted above, each applicant's employer must submit an affidavit containing a sworn representation to "make every effort" to avoid or eliminate any unauthorized pass usage, and to "strictly limit" all passes issued to personnel to carrying out the duties required and necessary in connection with the employer's contract with the agency. Historically, however, NYC Transit has not routinely provided the employers with the relevant usage data for their review. Rather, it is only in instances when a project manager identifies some potentially-unauthorized usage that the affected employer is provided with the relevant data for confirmation and reimbursement, if applicable.

In order to hold the employers more accountable for the unauthorized use of their employees' passes, it is essential that Security provide the employers with their employees' pass-usage data—on a regular basis—to review and certify that the passes are used for authorized purposes. Additionally, where despite receiving the relevant data the employers' compliance with their obligations is lax, and it is NYC Transit staff, not the contractor, who discovers the unauthorized usage, NYC Transit should consider the imposition of financial penalties on the employer in addition to requiring reimbursement.

Implementation of Applicant Background Check Requirement

Although the Policy requires Security to determine the appropriate level of background check required for each individual requesting access, it is silent as to who would be responsible for conducting such a background check if one is deemed necessary. Furthermore, there are no

[3] Adobe Portable Document Format (.PDF) or Plain Text File Format (.TXT)

guidelines on what actions should be taken if a contractor's employee is found to have adverse information in his or her background. As a result, Security has not made any such determinations or actually conducted any background checks. Security officials advised us that while they have been engaging in discussion with NYC Transit Law Department staff to develop guidelines to fully implement the Policy, the guidelines remain outstanding. Indisputably, securing NYC Transit properties, especially areas identified as "Critical Restricted" (e.g., tunnels, fan plants, ventilation buildings, signal/power rooms, etc.) is a function of paramount importance. In our view, therefore, NYC Transit must promptly and appropriately resolve this impasse.

RECOMMENDATIONS

NYC Transit should:

1. Make System Access and, when appropriate, MetroCard Temporary Transportation passes unusable on buses, unless the use of buses for MTA-related-business purposes is required and approved by a NYC Transit project manager.

   Agency Response: *"This recommendation has been fully implemented. As of May 2018, all System Access cards are unusableon buses. MetroCard Temporary Transportation cards are usable on buses and are only issued for MTA-related business purposes and require the written approval of theDepartment/Division head."*

2. Convert all System Access and MetroCard Temporary Transportation pass-usage data to a format that supports computerized screening and analysis to enhance the effectiveness and efficiency of the monitoring process.

   Agency Response: "This recommendation is fully implemented. We have already adopted some of the methodologies identified by your staff which has proved to be very helpful in finding unauthorized pass-usage."

3. Provide employers with pass-usage data on a regular basis to help them comply with the obligations they assumed when obtaining access passes for their employees.

   Agency Respoonse: *"This recommendation will be implemented commencing in the first quarter of 2019. In advance of the February pass renewal cycle, all vendors that will be requesting passes for their employees will be made aware of the new requirement of reviewing passusage data quarterly reports that they will receive from NYC Transit regarding their respective employees. This information will enable vendors to self-audit their employee's pass usage. This requirement will also be included in the new application packet provided to vendors."*

4. Consider the imposition of financial penalties on employers, in addition to requiring reimbursement, where despite receiving the relevant data the employers' compliance with their obligations is lax.

   Agency Response: "*This recommendation will be fully implemented in the first quarter of 2019. All our vendors/contractors will be informed that, in addition to being liable for any/all unauthorized swipe activity on their employees' access card, they may be subject to additional administrative fees.*"

5. Expedite the development of guidelines to implement the required background check of non-employee access pass applicant.

   Agency Response: "*The Department of Security has recommenced meetings with the Law Department to explore various options, which include coordinating with the MTA-agencies and/or regional partners. NYC Transit hopes to introduce a non-employee background check process by the end of the second quarter of 2019.*"

****

As always, we appreciate your attention to the issues we raised, as well as the courtesy and cooperation afforded to us at all times by your staff. Should you have any questions regarding this final report, please contact me or Executive Deputy Inspector General Elizabeth Keating at (212) 878-0022.

Very truly yours,

Barry L. Kluger

cc: Robert Diehl
John Martello
Kenneth Tobin