STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

CORRESPONDENCE MEMORANDUM

DATE: March 5, 2014

TO: Audit Committee Members

FROM: John Vincent, Director
Office of Internal Audit

SUBJECT: **Information Privacy or Security Incident Reporting Process Review (2013-08)**

This report is for Audit Committee review and discussion. No action is required.

Attached is the Executive Summary of the Information Privacy or Security Incident Reporting Process Review, which was completed and submitted to the Secretary of the Department of Employee Trust Funds. The Executive Summary provides the background, audit objectives and scope, findings, recommendations, and management's response. There are two recommendations in the report to which the Office of Policy, Privacy and Compliance (OPPC) has provided a management response.

The review was conducted in accordance with the biennial Audit Plan for 2013-2015. The review was performed to provide a reasonable assurance of employee adherence to Departmental policy for reporting unauthorized, inadvertent use, or disclosure of member personal information.

I will be available at the Audit Committee meeting to answer any questions.

Attachment: Executive Summary of the Information Privacy or Security Incident Reporting Process Review

Reviewed and approved by Robert J. Marchant, Deputy Secretary

Electronically Signed 3/13/14

Board	Mtg Date	Item #
AUD	3.27.14	6

STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax (608) 267-4549
http://etf.wi.gov

CORRESPONDENCE MEMORANDUM

March 5, 2014

Robert Conlin, Secretary
Department of Employee Trust Funds

AUDIT REPORT

Information Privacy or Security Incident Reporting Process Review (2013-08)

The Office of Internal Audit submits the final report of the Information Privacy or Security Incident Reporting Process Review.

The review was conducted in accordance with the biennial Audit Plan for 2013-2015. The review was performed to determine if the process for reporting the unauthorized, inadvertent use, or disclosure of member information is effective as designed.

The attached Executive Summary provides the background, audit objectives and scope, findings, recommendations, and management's response. There are two recommendations in the report to which the Office of Policy, Privacy, and Compliance responded.

Also, we greatly appreciate the assistance and cooperation of the Department's Privacy Officer, and the Office of Policy, Privacy, and Compliance during this review.

Respectfully submitted,

_____
John Vincent
Director, Office of Internal Audit

Cc: Rob Marchant, Deputy Secretary

STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax (608) 267-4549
http://etf.wi.gov

EXECUTIVE SUMMARY

Information Privacy or Security Incident Reporting Process Review (2013-08)

March 5, 2014

DEPARTMENT OF EMPLOYEE TRUST FUNDS

Information Privacy or Security Incident Reporting Process Review (2013-08)

EXECUTIVE SUMMARY

Introduction

The Department's *Information Security and Privacy Policy* under Section 14E of the Employee Trust Funds Work Policy Statement prohibits the unauthorized, inadvertent use, or disclosure of member personal information. The policy states the agency's position regarding maintaining the security of all confidential records, information, and actions which may be taken if an employee negligently or maliciously causes the unauthorized use or disclosure of member confidential information. One of the stated purposes of this policy includes the fact that certain types of personal information, such as data about a person's health condition, are subject to state and federal privacy laws that require specific actions before disclosure is permitted. Also that a breach of privacy can result in identity theft or benefits fraud. While certain member information may, by itself, not rise to the level of sensitive personal information, it becomes so when combined with other information. For these reasons, the Department requires that all employees report all incidences of unauthorized, inadvertent use, or disclosure of member personal information through their supervisors to the Privacy Officer for review and remediation.

Audit Objective

- Ensure that employees are following the Department's *Information Security and Privacy Policy* on reporting the unauthorized, inadvertent use or disclosure of member confidential personal information to the Department's Privacy Officer for review and remediation, if required.

Audit Scope

- Confirm employees' adherence to the Department's policy for reporting incidences of unauthorized, inadvertent use, or disclosure of members' confidential information to the Privacy Officer for review and remediation.
- Interview division directors and supervisors on their adherence to the Department's privacy policy and procedures used for filing incident reports.
- The period for this review is from January 1 to June 30, 2013.

Summary of Findings

The Department's *Information Security and Privacy Policy* requires all employees to report unauthorized, inadvertent use or disclosure of member confidential personal information to the Department's Privacy Officer for resolution. Our review showed that employees are following this policy and reported 25 incidents to the Privacy Officer between January and June 2013. The reported incidents were the result of human errors in the normal course of business related to computer keying and the collating member information packets prior to mailing. At times, the process of assembling and

mailing member information packets exceeds 260 pieces of mail per day. Therefore, the process is susceptible to human error -- albeit a very small percentage when compared to annual total mail volume.

We found no evidence where a computer keying or packet collating/mailing prep error resulted in a member's identity theft or fraud. The Department has since retrained staff involved in packet collating/mail prep and implemented additional layers of controls to include using member identification, last and first names, and the last six digits of a participant's social security number. Responsible computer keying staff were retrained and are being monitored for accuracy by their respective supervisors. The reported incidences are shown below:

January to June 2013 Incidence Report

Incidence Type	1st Quarter (Jan-Mar)	Percentage of Q1Total	2nd Quarter (Apr-Jun)	Percentage of Q2 Total	Total
Mailing	8	47%	4	50%	12
Computer Keying	8	47%	2	25%	10
Automatic National Change of Address	1	6%	2	25%	3
Total Count	17	100%	8	100%	25

Conclusion

Employees' human errors accounted for the majority of the incidents reported during this review. All 25 incidents were reported in a timely way to the Department's Privacy Officer for investigation, appropriate corrective actions were taken, and affected parties notified. The division responsible for member information packets implemented extra mail prep procedures to prevent future errors. Additionally, supervisors retrained certain employees involved with computer keying errors and are monitored for work accuracy. In conclusion, while human errors may not be completely eliminated or caught at the point of infraction, the process in place for notifying the Department's Privacy Officer is effective and working as designed.

Observation

The Office of Internal Audit notes the Department has only one designated Privacy Officer, with no designated secondary or back up officer. In addition, the Privacy Officer's other functions include: research and analysis on proposed legislation and policy changes; drafting statutes and administrative rules; and other functions that require significant allocation of time away from privacy/security issues. Based on the significant role of the agency's privacy officer, the Office of Internal Audit feels it would be advantageous to formally designate a secondary staff member to assist the primary

Privacy Officer, especially when on vacation, occupied with legislative or compliance activities, or out of the office.

Recommendations and Management Response

Recommendation 1 – The Department should designate a secondary Privacy Officer to prevent the void created by vacation, sick day, or the primary Privacy Officer's legislative and compliance duties.

> *Management Response -- The Director of the Office of Policy, Privacy and Compliance (OPPC) fills in for any OPPC staff who are absent. The Director will continue to serve as the secondary Privacy Officer as needed or will designate a person to serve as a secondary Privacy Officer. The Director and the Privacy Officer will establish written protocols and training for the secondary Privacy Officer during the second quarter of 2014.*

Recommendation 2 – The OPPC should create a Privacy E-mail inbox. Such a Privacy e-mail inbox would allow both the primary and secondary Privacy Officers to monitor the incident reports submitted to that site.

> *Management Response - The OPPC Director will contact the Bureau of Information Technology Services by March 14, 2014, to create an e-mail inbox specifically for Information Privacy or Security Incident Reports. This inbox would be accessed by the Director, the Privacy Officer and the Secondary Privacy Officer.*