Date: August 23, 2013

To: Dr. Ashok Roy, Vice President for Finance and Administration

Cc: Sandra Culver, Associate Vice Chancellor, Financial Services – UAA
Raaj Kurapati, Associate Vice Chancellor, Financial Services – UAF
Tom Dienst, Director Business Services - UAS

From: Dr. Russ O’Hare, Chief Records Officer

RE: 2013 Red Flag UA Identity Theft Prevention Program Report

The University of Alaska (UA) Identity Theft Prevention Program (Red Flags) states that “... at least annually university staff responsible for the administration of the program shall report to the Program Administrator on program compliance.” This memorandum provides a summary of program information provided by representatives from UAA, UAF, and UAS.

- There were no reported instances of suspicious activities of covered accounts or incidents of identity theft.
- The MAU’s report the program procedures have strengthened the protection of the university’s customer information.
- There are no recommendations for modifying the program at this time.

Additional information and recommendations follow:

- During FY 13, the Chief Records Officer and the SW Director for Faculty/Staff Training & Development collaborated in the development and implementation of an online version of the UA Identity Theft Prevention Program Training. Thus, allowing employees to access the Identity Theft Prevention Training via UA Online.
- UAS noted experiencing a small number of cases where the identity of individuals requesting student FERPA protected information could not be verified when challenge questions were posed. Information was not released. (This is not specific to FTC Red Flag Identity Theft protection of “covered accounts”.)
- UAS would like to see integrated training on protection of personally identifiable information (PII) that combines legislative and compliance standards of FERPA, HIPPA, HEOA, FTC, and PCI-DSS.
• UAF representatives developed a streamlined version of the UA Identity Theft Prevention Program to provide awareness and familiarization for their employees who do not regularly access or handle covered accounts.

• UAS recommends UA develop a system generated alert email that would be issued to the owner of personally identifiable information when his or her information is updated online in Banner through any of the self-service web based features.

• UAF recommends identifying job families where responsibilities would include access to and handling of sensitive information and expect that employees who fall into these families be required to take the identity theft prevention training.

• UAF recommends that identity theft training be offered as part of the mandatory training expected during the employee on-boarding process.