Precautions to Help You Avoid Telephone, Computer or Email Fraud

- Be suspicious of unsolicited phone calls, requests, or email messages from individuals asking about you, other APS employees or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify the person's identity directly with the company.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known "phishing" attacks is also available online from groups such as the Anti-Phishing Working Group at http://www.antiphishing.org.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. For more information, see *Understanding Firewalls*, http://www.us-cert.gov/ncas/tips/ST04-004; *Understanding Anti-Virus Software*, http://www.us-cert.gov/ncas/tips/ST04-005; and *Reducing Spam*, http://www.us-cert.gov/ncas/tips/ST04-007.
- Regularly clear your browsing history, cache and cookies. Information on how to do that for all mobile and desktop browsers is available at https://kb.iu.edu/d/ahic.
- Do not use the same password for every login. As an added safeguard, you also should frequently change your passwords.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.
- The IRS also provides all taxpayers helpful suggestions at https://www.irs.gov/uac/Newsroom/How-New-Identity-Security-Changes-May-Affect-Taxpayers-for-2016

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.Identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You can place a "fraud alert" on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.