ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT

Safeguarding Signature Mechanisms

December 2016

Why are we issuing this alert?

The unauthorized use of signature mechanisms can lead to the theft and misuse of public monies. In fact, we recently issued a report detailing a fire district employee's misuse of signature stamps resulting in that employee embezzling nearly $1.8 million dollars of public monies.[1] This employee was indicted on 25 felony charges. However, effective controls over signature mechanisms could have helped prevent this embezzlement. This alert outlines how public officials can help protect public monies and deter and detect fraud by developing and implementing policies and procedures regulating the use of signature stamp mechanisms; restricting the use of these mechanisms to the person whose signature is represented; and ensuring the appropriate segregation of duties for those employees who have access to these mechanisms.

What are signature stamps and electronic signatures?

Signatures are used to document an individual's knowledge and approval. However, an individual's signature does not need to be inked and handwritten to be legally binding. Public entities use a combination of nonhandwritten signatures like signature stamps and electronic signatures. Signature stamps and other nonelectronic facsimile signatures replicate a handwritten signature. Conversely, electronic signatures use various methods to authenticate an electronic record, such as those included in an email, initials added to a spreadsheet, a personal identification number entered in a bank's automated teller machine, and a signature for a credit or debit card purchase done on a digital pen pad service.

Signature mechanisms include:

- Signature stamps, such as a rubber stamp.
- Electronic signatures, such as email and digital signatures. Digital signatures are more secure because they use encryption methods to ensure the document's integrity and authenticity, and prevent the electronic signature from being copied to another document. For instance, a digital signature could be used to further secure email by obtaining what is known as a certificate from a reputable third party that has verified the authenticity of a user's email account. This certificate can then be used to sign and encrypt future email communications that are tied to that user's validated email address. This will inform the recipient that the communication was received from the stated user.

For signature stamps, public officials should ensure that there is adequate control of all stamps and that stamps are restricted to authorized personnel, including only to the person whose signature is represented. For electronic signatures, Arizona Revised Statutes §18-442 prescribes rules governing documents filed with or by a state agency, board, or commission containing these signatures. Specifically, the rules state that an electronic signature should be unique to the person using it, capable of reliable verification, and linked to a record in a manner such that if the record is changed, the electronic signature becomes invalidated.

Public officials and employees use the above signature mechanisms in various ways, including to electronically authorize payment and payroll vouchers, approve purchase orders, sign checks, and publish hard copy and electronic versions of reports. When used properly, these signature mechanisms can be used to expedite the approval process and provide an adequate audit trail in the digital age.

---

[1] See Office of the Auditor General, Special Investigation: *Show Low Fire District—Theft and Misuse of Public Monies*, May 2016, Report No. 16-402.

Inadequate oversight and controls can lead to the misuse of signature mechanisms

If adequate controls are not implemented to safeguard and restrict access to these signature mechanisms, employees can more easily authorize fraudulent expenditures and sign checks, ultimately leading to the theft and misuse of public monies. As described on the first page, our Office reported in May 2016 that an Arizona fire district allowed an employee unrestricted access to governing board members' signature stamps, check stock, check-register-accounting software, and bank statements. The employee regularly used these stamps without board members' review or approval, sometimes using a stamp 23 months after the member had served on the governing board. With access to the governing board members' stamps, the employee was able to unlawfully issue checks payable in her name, her father's name, and her then-fiancés' name, and also to credit card accounts associated with these same individuals, resulting in her embezzlement of $1,794,595 of public monies. This employee was later indicted by the Navajo County Grand Jury on 25 felony counts related to theft, misuse of public monies, fraudulent schemes, computer tampering, forgery, false filing, conspiracy, illegally conducting an enterprise, assisting a criminal syndicate, and money laundering.

Additionally, during an investigation of an Arizona school district, our Office reported in March 2013 that a district administrator allowed an employee unrestricted access to his signature stamp and computer login credentials.[2] Consequently, the administrator failed to provide adequate oversight of the employee's purchasing activities, which created a deficiency in this district's internal controls. With access to the administrator's signature stamp and login credentials, the employee was able to approve personal expenditures she made on the administrator's purchasing card and misuse $32,501 of public monies. This employee was later indicted by a State Grand Jury on felony counts related to theft, misuse of public monies, fraudulent schemes, and forgery.

Appropriate oversight and controls help prevent unauthorized use of signature mechanisms

Public officials should exercise their fiduciary responsibility to help protect public monies by establishing and enforcing fundamental controls over these signature mechanisms, such as:

- Developing and implementing policies and procedures regarding their purposes and how they should be used.
- Restricting their use to the person whose signature is represented, securely storing stamps, and protecting electronic signatures with passwords and encryption methods.
- Ensuring that each electronic signature is unique to the person using it, capable of reliable verification, and linked to a record in a manner such that if the record is changed, the electronic signature becomes invalidated.
- Maintaining adequate segregation of duties by prohibiting employees who have the authority to sign checks with or without signature mechanisms from having access to blank check stock or preparing checks and prohibiting check signers from initiating and approving entire transactions, such as approving their own purchases.

[2] See Office of the Auditor General, Special Investigation: *Glendale Elementary School District—Theft and Misuse of Public Monies*, March 2013.