

FILED
4:45 O'clock *P.M.*

MAR 6 2019 ✓

DONNA McQUALITY, Clerk
 By: J DEROIS

IN THE SUPERIOR COURT OF ARIZONA
 IN AND FOR THE COUNTY OF YAVAPAI

IN THE MATTER OF: _____)
 PROVIDING NOTIFICATIONS IN THE EVENT) ADMINISTRATIVE ORDER
 OF BREACH OF COMPUTER SECURITY)
 SYSTEM CONTAINING PERSONAL) NO. 2019-03
 INFORMATION)
)
)

This procedure provides direction for performing various notifications in the event of a loss of a computer or personal storage device or breach of a computer security system containing personal information as defined by A.R.S. § 18-551.

As revised, A.R.S. § 18-551 defines "Personal Information" to mean an individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account **or** first name or first initial and last name in combination with any one or more data elements, when the data element in not encrypted, redacted, or secured by any other method rendering the element unreadable or unusable:

- a. An individual's social security number.
- b. The number on an individual's driver license or nonoperating identification license.
- c. A private key that is unique to an individual and that is used to authenticate or sign an electronic record.
- d. An individual's financial account number or credit or debit card number in combination with any security code, access code, or password that would allow access to the individual's financial account.
- e. An individual's health insurance identification number.
- f. Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional.
- g. An individual's passport number.
- h. An individual's taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service.
- i. Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account.

()
 ()
 ()
 ()
 ()
 ()
 () Other _____

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

"Breach", "breach of a computer security system", or "security breach" means an unauthorized acquisition of and access to unencrypted or un-redacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information regarding multiple individuals. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security system if the personal information is not used for a purpose unrelated to the person or subject to further unauthorized disclosure.

"Portable storage devices" means flash-memory-based "thumb" or "jump" drives, personal phones, or external hard drives. It also includes any offsite data repository or cloud storage location other than the court's OneDrive for Business.

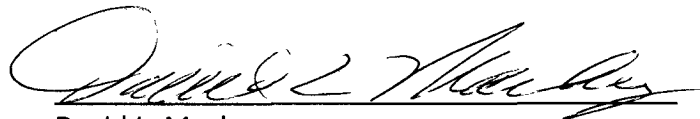
For the reasons cited above, IT IS HEREBY ORDERED that:

1. A court, clerk, or probation employee who first learns of the actual loss or security breach or event having the potential of perpetrating a breach shall notify his or her immediate supervisor and provide details of loss or breach immediately upon discovery. Loss can include portable storage devices as well as portable computers. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.
2. The immediate supervisor of the employee reporting actual loss or data breach or potential breach shall notify local Clerk of Court and Court Administrator, as well as the Clerk of Court and Court Administrator of any other court whose data may likely have been lost or compromised without delay.
3. The Court Administrator or Clerk of Court responsible for the data impacted by the loss or breach shall verify whether a breach or loss has actually occurred along with the scope of the damage and notify the presiding judge of the court. When necessary, conduct an investigation with law enforcement or a third-party forensic auditor as quickly as possible.
4. The Presiding Judge, Court Administrator, or Clerk of Court responsible for the data impacted by the loss or breach shall notify the Chief Information Officer at the Administrative Office of the Courts Information Technology Division (602-452-3350), and the Administrative Director of the AOC (602-452-3307), by phone or high priority e-mail within 24 hours of being notified of the loss or breach.
5. When law enforcement or a third-party auditor is involved, seek their advice about whether notification to affected persons would negatively impact a criminal investigation.
6. Court Administrator or Clerk of Court responsible for the data impacted by the loss or breach shall draft communication to affected persons using the content of sample letters attached to Supreme Court AO 2018-72 as soon as possible. No communication shall be released until law enforcement or the third-party auditor provides authorization to publicize the loss or breach, but it must then be made within 45 days of that determination.

7. Communication shall be made in writing to each individual affected but may be accomplished via e-mail where accurate addresses exist for those who are subject to notification. Direct telephonic contact is allowable as long as no prerecorded message is employed.
8. When the loss or breach affects over 1,000 people, the court shall coordinate communication to the three largest nationwide consumer reporting agencies and notify the Arizona Office of the Attorney General.
9. When more than 100,000 people are affected by the loss or breach or the cost of notification is above \$50,000, or when insufficient contact information exists, the draft communication shall be forwarded to the Administrative Office of the Courts Executive Office. AOC's Public Information Officer will communicate appropriate notice using the azcourts.gov website for a minimum of 45 consecutive days and inform the Arizona Attorney General's Office of the facts necessitating substitute notice via the website.
10. When the breach involves only an individual's user name or e-mail address in combination with a password or security question and answer for online account access, the password must be reset immediately and notification needs only to contain the information in Sample Letter 4 attached to Supreme Court AO 2018-72.

IT IS FURTHER ORDERED that this policy shall apply to the Adult Probation Division, Juvenile Court Services, the Clerk of Court and Justice Courts in Yavapai County and may apply to the Municipal and Magistrate Courts in Yavapai County if so adopted.

Dated this 5th day of March, 2019.



David L. Mackey,
Presiding Judge of the Superior Court

Copies: Court Administration
Clerk of Court
Adult Probation Department
Juvenile Court Services
5 Justice Courts
9 Muni/Mag Courts