FILED
AMANDA STANFORD
CLERK OF SUPERIOR COURT

18 OCT 30 PM 1:53

AL

BY _____
DEPUTY

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF PINAL

IN THE MATTER OF PROTECTING THE PERSONAL INFORMATION OF COURT USERS AND NOTIFYING AFFECTED PERSONS IN THE EVENT OF A BREACH OF THE SECURITY SYSTEM	ADMINISTRATIVE ORDER No. 2018 - 00034 (Amending No. 2008-54)

WHEREAS, a duty is imposed upon the courts to safeguard certain personal information required to be provided by individuals who have business with the Courts; and

WHEREAS, such personal information is recorded and retained by the Courts in a variety of media including computerized data bases; and

WHEREAS, Administrative Order 2018-72 (which replaced Administrative Order 2008-68) was issued by the Chief Justice, Supreme Court of Arizona, August 18, 2018, directing all courts, on or before January 1, 2019 to revise their local policy protection of databases containing confidential personal information;

IT IS HEREBY ORDERED as follows:

That all courts, clerks, court employees, probation officers and other staff, situate in Pinal County, Arizona, which are subject to the administrative directives of the Presiding Judge, Superior Court, shall comply with the procedures for reporting and providing notification of breaches and potential breaches of security regarding confidential personal information as set forth in the attachment hereto;

IT IS FURTHER ORDERED, that all court clerks, deputy clerks, court employees, probation officers and other staff shall be informed of and instructed on their duties pursuant to the procedures adopted hereby and attached hereto.

DATED this 30th day of October 2018.

[redacted]

HONORABLE STEPHEN F. MCCARVILLE,
PRESIDING JUDGE

Original: Clerk of the Superior Court
Copies: Superior Court Judges
Todd Zweig, Court Administrator
Denise Smith, Juvenile Court Services
Rod McKone, Adult Probation
Tracy McElroy, Conciliation Court Director
Amanda Stanford, Clerk of the Court
Odette Apodaca, Court Services Program Manager

JP

Purpose

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.

Definitions

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.

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.

Procedure

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 Karl Heckart at the Administrative Office of the Courts Information Technology Division (602-452-3350), and Dave Byers, 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 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 AO 2018-72.

Implementation of Administrative Order 2018-72, Notice to Affected Persons in the Event of Breach or Disclosure of Unencrypted Computer Data

Guidance for creating a local court policy applicable to local automation systems and locally stored data

Responsible Role	Action Required by Policy	Timeframe/Qualifier
Court, clerk, or probation employee who first learns of the actual loss or data breach or potential breach	Notify immediate supervisor and provide details of loss or breach	Immediately upon discovery
Immediate supervisor of employee reporting actual loss or data breach or potential breach	1. Notify local Clerk of Court and Court Administrator, and 2. Notify Clerk of Court and Court Administrator of any other court whose data may likely have been lost or compromised.	Without delay
Court Administrator or Clerk of Court responsible for the data impacted by the loss or breach	1. Verify whether a breach or loss has occurred and scope of damage, 2. Notify Presiding Judge, 3. Notify Karl Heckart at AOC ITD (602-452-3350), and Dave Byers, Administrative Director of the AOC (602-452-3307), by phone or high priority e-mail, and 4. Notify applicable local law enforcement agency or forensic auditor.	Within 24 hours
Law enforcement / Forensic auditor	Advise local Court Administrator, Clerk of Court and Presiding Judge whether notification to affected persons would negatively impact criminal investigation.	As scope of loss is determined
Court Administrator or Clerk of Court responsible for the data impacted by the loss or breach	Draft communication to affected persons using content of sample letters attached to AO 2018-72 as guideline.	As soon as possible, once extent of loss or breach is clearly understood and law enforcement advises investigation won't be affected
Court Administrator or Clerk of Court responsible for the data impacted by the loss or breach	Provide notification to affected parties within 45 days of determination that a breach or disclosure has occurred if < 100,000 people affected or cost of notification is < $50,000.00. Inform AZ Attorney General's Office. OR Provide details to AOC Executive Office if >100,000 people affected or cost is >$50,000 or insufficient contact details exist to perform notice. AOC will inform AZ Attorney General's Office.	As soon as possible

Responsible Role	Action Required by Policy	Timeframe/Qualifier
AOC Executive Office	1. Notify State Information Security & Privacy Office at ADOA-ASET, and 2. Communicate notice conspicuously on azcourts.gov website for 45 days minimum.	Without delay

IN THE SUPREME COURT OF THE STATE OF ARIZONA

In the Matter of: PROTECTING THE PERSONAL INFORMATION OF COURT USERS AND NOTIFYING AFFECTED PERSONS IN THE EVENT OF A SECURITY SYSTEM BREACH	Administrative Order No. 2018 - 72 (Replacing Administrative Order No. 2008-68)

Administrative Order No. 2008-68 issued by this court required creation and adoption of a local policy for protection of confidential personal information and notification of affected persons in the event of a breach that exposes unencrypted or unredacted personal information not otherwise publicly available. A.R.S. § 18-552(O) requires courts to "create and maintain an information security policy that includes notification procedures for a security system breach" of the court. A.R.S. § 18-551(1) defines a security system breach as follows:

> An unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information maintained as part of a database of personal information regarding multiple individuals.

Personal information about court users is collected in the course of conducting the official business of the judiciary as required by law or as necessary or desirable to carry out judicial orders. Recent legislative changes (Law 2018, Ch. 177, HB 2154) have expanded the definition of personal information to include both of the following:

> (i) An individual's first name or first initial and last name in combination with one or more specified data elements.
> (ii) 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.

A.R.S. § 18-551(7)(a).

HB 2154 also greatly expanded the definition of "specified data element" to include any of the following:

> (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.

A.R.S. § 18-551(11).

The protection of confidential personal information and notification of affected persons in the event of a breach is of paramount importance to the public and the judiciary. Statewide policies are needed to define responsibility for notifying individuals who may be affected when the security of their personal information has been compromised.

Therefore, pursuant to Article VI, Section 3, of the Arizona Constitution,

IT IS ORDERED that not later than January 1, 2019, all courts shall revise their local policy complying with Administrative Order No. 2008-68 requiring protection of databases containing confidential personal information to incorporate the expanded definition of personal information in A.R.S. § 18-551(7) and (11). The Administrative Office of the Courts (AOC) shall revise the policy for the automation systems and centralized data it manages, with which courts using statewide systems will be expected to comply. Any individual court managing a local automation system or storing data locally or in the cloud shall adopt a policy governing security of those databases. At a minimum, the revised policies shall include:

1. **Responsibility for judicial department notification.** Any court employee who downloads all or part of a database of confidential personal information regarding multiple individuals onto an end-user storage device other than a court computer or court-provided mobile device, shall provide notice to his or her supervisor or other appropriate person in the chain of authority if a breach may have occurred. An end-user storage device may include a personal PC, phone, or flash drive, or an off-site data storage system such as a web-based data repository or "cloud storage" location other than the court's OneDrive for Business. The court administrator or clerk of court responsible for the data system that is suspected of being breached shall notify the presiding judge of the court and the Administrative Director within 24 hours.

2. **Breach notification procedures.** The court administrator or clerk of court responsible for the automated system or storage device that is the object of the suspected breach shall determine whether a breach has occurred and notify those affected if a breach has occurred. The person responsible for providing notice of the breach shall provide the required notice in the most expeditious manner possible and without delay, subject to the needs of law enforcement if a criminal investigation is pending, and within 45 days of the positive determination of the breach. Sample notification letters are attached to this order. e-Mail notices may be used where the court has addresses. Telephonic notice may be used if contact is made directly with the affected individuals and not through a prerecorded message.

3. **Large scope notification instructions.** When more than 1000 individuals are affected, the court must also notify the three largest nationwide consumer reporting agencies and the Arizona Attorney General's Office as required by § 18-552(B)(2)(b). When the cost of individual notices exceeds $50,000.00 or the breach affects more than 100,000 individuals, the local court shall coordinate such notification through the AOC, which shall notify the public using conspicuous posting of the notice on the AZCourts.gov website for at least 45 days and shall provide written notice to the Arizona Attorney General's Office as required by § 18-552(F)(4)(a).

Dated this 8th day of August, 2018.

SCOTT BALES
Chief Justice

SAMPLE LETTER 1
Data Acquired: Credit Card Number or Financial Account Number Only

Dear :

We are writing to you because of a recent incident involving a breach of security for an electronic database at [*name of court or department*] containing [*specific category of personal information*] on [*approximate date*].

[*Describe what happened in general terms, what type of personal information was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact the credit card or financial account issuer for the account that may have been the subject of unauthorized access and ask them to either close your account or provide you with a new account number. Tell them that your account may have been compromised. If you want to open a new account, ask the company to give you a PIN or password. This will help control access to the new account in the future.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number or address below.

Experian	Equifax Information Services	TransUnion
888-397-3742	888-766-0008	800-680-7289
475 Anton Blvd.	P. O. Box 740256	P.O. Box 2000
Costa Mesa, CA 92626	Atlanta, GA 30374	Chester, PA 19016

For more information on identity theft, we suggest that you visit the Office of the Attorney General at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft or (202) 326-2222 or 600 Pennsylvania Avenue, NW, Washington, DC 20580. If there is anything [*name of department*] can do to assist you, please call [*phone number*].

[*Closing*]

SAMPLE LETTER 2
Data Acquired: Driver's License or Arizona ID Card Number

Dear :

We are writing to you because of a recent incident involving a breach of security for an electronic database at [*name of court or department*] on [*approximate date*].

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

Since your Driver's License [*or Arizona Identification Card*] number was involved, we recommend that you immediately contact your local Dept. of Motor Vehicles office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free MVD Customer Service Center at 800-251-5866 for additional information.

If your Driver's License or Arizona ID Card Number is also your Social Security Number, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them with instructions on how to get a free copy of your credit report from each.

Experian	Equifax Information Services	TransUnion
888-397-3742	888-766-0008	800-680-7289
475 Anton Blvd.	P. O. Box 740256	P.O. Box 2000
Costa Mesa, CA 92626	Atlanta, GA 30374	Chester, PA 19016

Look over your credit reports carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Look for personal information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Office of the Attorney General

at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft or (202) 326-2222 or 600 Pennsylvania Avenue, NW, Washington, DC 20580. If there is anything [*name of your department*] can do to assist you, please call [*phone number*].

[*Closing*]

SAMPLE LETTER 3
Data Acquired: Social Security Number or Taxpayer Identification Number

Dear :

We are writing to you because of a recent security incident at [*name of court or department*] that took place on [*approximate date*]. [*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax Information Services	TransUnion
888-397-3742	888-766-0008	800-680-7289
475 Anton Blvd.	P. O. Box 740256	P.O. Box 2000
Costa Mesa, CA 92626	Atlanta, GA 30374	Chester, PA 19016

Look over your credit reports carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Office of the Attorney General at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft or (202) 326-2222 or 600 Pennsylvania Avenue, NW, Washington, DC 20580. If there is anything [*name of your department*] can do to assist you, please call [*phone number*].

[*Closing*]

SAMPLE LETTER 4

Data Acquired: User Name or e-Mail Address with Password or Security Question/Answer

Dear :

We are writing to you because of a recent incident involving a breach of security for an electronic database storing your login credentials for an online application at [*name of court or department*] on [*approximate date*].

[*Describe what happened in general terms, what specific information was involved, and what you are doing in response.*]

We have forced a password reset for your account effective upon your next login. To protect yourself from the possibility of other online accounts having matching user IDs and passwords or security questions/answers being taken over, we recommend that you immediately change passwords and security questions for any website that makes use of the same user name, password, or security questions/answers.

Protection of your online account information is a high priority for us. If there is anything [*name of department*] can do to further assist you, please call [*phone number*].

[*Closing*]