

IN THE SUPREME COURT OF THE STATE OF ARIZONA

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

A. R. S. § 44-7501(K) requires courts to “create and maintain an information security policy that includes notification procedures for a breach of the security system” of the court. The statute defines a breach as follows:

[A]n unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained . . . as part of a database of personal information regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual. A.R.S. § 44-7501(L)(1).

Personal information about court users is collected in the course of conducting the official business of the judiciary as required by law or to carry out judicial orders. The sometimes centralized and sometimes decentralized nature of court computing resources necessitates guidance regarding responsibility for protection of court data pursuant to § 44-7501(K), especially data that identifies individual court users. The increased portability of end-user storage devices enables centrally-managed data to be copied onto portable devices and transported offsite. The high cost of encrypting data makes it impractical as an across-the-board solution. Therefore, statewide policies are needed to define responsibility for notifying individuals who may be impacted when court data security is compromised.

Now, therefore, pursuant to Article VI, Section 3, of the Arizona Constitution,

IT IS ORDERED that all courts adopt a policy requiring protection of court users’ electronic personal information including a provision for notifying affected persons in the event of a breach in the court security system that exposes unencrypted or unredacted personal information. At a minimum, the court’s policy shall provide the following provisions:

1. Responsibility for breach notification pursuant to § 44-7501. The individual in possession of or otherwise responsible for the automated system or storage device that is the object of the breach shall be responsible for notifying those impacted that the breach has occurred. For example, the Administrative Office of the Courts (AOC) would provide notice in the case of a breach of data on the equipment maintained by the AOC, a local court or clerk of court, as appropriate, would provide notice in the case of a breach of the local court’s computer or computer

server. Any court employee who downloads official court data onto an end-user storage device such as a personal PC or flash drive, or onto an off-site data storage system, such as a web-based data repository, shall be solely responsible for providing notice of the breach.

2. Breach notification. The individual or entity 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. Notification to the public shall contain:

- a. A general description of what occurred;
- b. The nature of personal information involved;
- c. Steps taken to protect personal information from further unauthorized acquisition or access;
- d. A recommendation to notify credit reporting agencies (Equifax, Experian, and TransUnion) for fraud alert; and
- e. Availability of information concerning identity theft from the Arizona Office of the Attorney General and/or Arizona Department of Public Safety websites.

The person or entity responsible for providing notice shall also notify the presiding judge and clerk of court, if any, of the court whose data has been compromised as well as the AOC Information Technology Division, and the Administrative Director in the most expeditious manner possible.

In situations where the cost of individual notices exceeds \$50,000.00 or the breach affects more than 100,000 persons, AOC shall notify the public through the Executive Office using statewide media outlets.

Sample notification letters have been attached to this order for court use.

Dated this _____ day of _____, 2008.

RUTH V. MCGREGOR
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]*.

[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.

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. 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]*.

[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	TransUnion
888-397-3742	800-525-6285	800-680-7289

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. 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

Dear :

We are writing to you because of a recent security incident at *[name of court or department]*. *[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
888-397-3742

Equifax
800-525-6285

TransUnion
800-680-7289

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. If there is anything *[name of your department]* can do to assist you, please call *[phone number]*.

[Closing]