

**Alaska Department of Health and Social Services  
Frequently Asked Questions - Data breach**

**1. What happened?**

A computer device was stolen from a department employee and may or may not involve the loss of personal information of Alaskans served by the Department of Health and Social Services. The device, a 120 gigabyte portable hard drive, was used amongst computer technicians moving state employee information from old computers to new computers.

**2. When did it happen?**

The theft occurred on October 12th. Upon investigation, it was determined the device might contain computer data from several divisions within the department. The department's investigation into what may have been on the stolen device is still ongoing, and any parties who may have had information breached will be notified.

**3. Why did you have my personal information?**

The department has information on Alaskans who use various health and social services programs to ensure their eligibility and to effectively deliver services.

**4. What specific items of my personal information were involved?**

It is unclear whether individual Alaskans personal information was on the stolen device. It is possible that no Alaskan's personal information was on the device, but the department takes the security of such information very seriously and wanted to ensure that Alaskans were warned of the possibility.

**5. What are you doing about the breach? How will you prevent this from happening in the future?**

DHSS is reviewing the breach to help determine what information may have been on the stolen device. The department plans to send a notice to Alaskans who receive services as a precaution. The notice will recommend actions that Alaskans can take to protect their identity, such as placing a freeze on their credit report.

The Department is also securing all current software applications by changing passwords and updating the security to ensure that no stolen employee information may be used to compromise these applications.

To prevent further breaches, DHSS has adopted the Department of Administration, Enterprise Technology Services standard security product, Guardian Edge, which will protect information stored on portable devices. DHSS has already deployed the solution to all devices used by IT Services staff.

**6. How are you alerting people who might have had their information breached?**

DHSS is being proactive in alerting Alaskans, even if their information may not have been on the device that was stolen. The department is taking the following steps:

- Alerting statewide media
- Placing a notice on the department website at [hss.alaska.gov/security](http://hss.alaska.gov/security)
- Alerting stakeholders and partner organizations
- Sending a notice to Alaskans who receive services from the department
- Setting up a hotline to answer questions from those who are concerned

- Alerting the U.S. Department of Health and Human Services Secretary

**7. Does this mean that I'm a victim of identity theft?**

No. The fact that someone may have had access to your information doesn't mean that you are a victim of identity theft or that your information will be used to commit fraud. We are notifying Alaskans about the incident so that they can take appropriate steps to protect themselves. The first step to take is to place a fraud alert on credit files, order credit reports and review them for possible problems.

If you do not receive services from the Alaska Department of Health and Social Services, it is extremely unlikely that your personal information was compromised.

**8. How will I know if any of my personal information was used by someone else?**

The best way to find out is to order credit reports from the three credit bureaus: Equifax, Experian and Trans Union. Look for accounts on credit reports that were not authorized or applications for credit ("inquiries") that you did not make, these could be indications that someone else is using your personal information without your permission.

**9. Do I have to pay for the credit report?**

No. You can order your credit reports from all three credit bureaus for free once a year. You can do this online at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by phone at 1-877-322-8228.

**10. What else can I do to protect myself?**

You can place a fraud alert on your credit files. Simply call any one of the three credit bureaus at the numbers provided below and follow the "fraud victim" instructions. The one you call will notify the others to place the alert. When you call the credit bureau fraud line, you will be asked for identifying information and will be given the opportunity to enter a phone number for creditors to call. You may want to make this your cell phone number.

- **Trans Union – 1-800-680-7289**
- **Experian – 1-888-397-3742**
- **Equifax – 1-800-525-6285**

**11. What should I look for on my credit report?**

Look for any accounts that you don't recognize, especially accounts opened recently. Look at the inquiries or requests section for names of creditors from whom you haven't requested credit. Note that some kinds of inquiries, labeled something like "promotional inquiries," are for unsolicited offers of credit, mostly from companies with whom you do business.

Don't be concerned about those inquiries as a sign of fraud. (You are automatically removed from lists to receive unsolicited pre-approved credit offers when you put a fraud alert on your account. You can also stop those offers by calling 888-5OPTOUT.)

Look in the personal information section for addresses where you've never lived. Any of these things might be indications of fraud. Also be on the alert for other possible signs of identity theft, such as calls from creditors or debt collectors about bills that you don't recognize, or unusual charges on your credit card bills.

**12. What happens if I find out that I have been a victim of identity theft?**

You should immediately notify your local law enforcement agency, contact any creditors and

notify the credit bureaus. More information on identifying and responding to identify theft can be found on this Department of Justice web site:

<http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>.

**13. Were the police notified?**

DHSS has notified law enforcement and will be cooperating with any ongoing investigation.

**14. Any suspects?**

No, there are no suspects at this time.

**15. Who was the employee?**

We cannot reveal details about the incident or who was involved during an official investigation

**16. Was the employee conducting state business at the time?**

No, the incident was not during the employee's work hours.

**17. Where did this theft occur exactly?**

The employee reported the theft took place at a convenience store. More details are not available since this is an ongoing investigation.

**18. What kind of information are we talking about, credit cards, SS #s, addresses, medical information?**

Potentially, the information on the stolen device may contain names, addresses, Social Security numbers, dates of birth, and medical information.

**19. Has this happened before?**

While the department has suffered lost or stolen equipment in the past, this particular instance is being handled differently because of the potential for personal information being on the stolen device. The department is handling this situation very carefully and is taking efforts to inform Alaskans so that they may take proactive steps to monitor and ensure they are not victims of identity theft.

**20. What are the laws concerning this?**

There are two primary laws pertaining to the breach of personal information. The Alaska Personal Information Protection Act and the federal Health Insurance Portability and Accountability Act.