

Model Letter to Affected Individual of Breach of Security of Data

IMPORTANT NOTICE OF [IDENTIFIED INCIDENT]

Dear <>:

You are receiving this letter because a recent incident at <College/university> may have [exposed you to identity theft or describe other potential, serious consequence of incident, if applicable].

[Describe what happened in general terms; what kind of private or confidential information was involved, and steps the college/university is taking in response.]

If breach involved data that could be used for identity theft such as: name and SSN, credit card or financial account number include the following:

<College/university> is writing to you so that you can take steps to protect yourself from the possibility of identity theft.

Include this paragraph if credit card number or other financial account number: The Federal Trade Commission (FTC) recommends that you immediately contact [credit card or financial account issuer] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask the account issuer to give you a PIN or password to help control access to the account.

The Federal Trade Commission (FTC) recommends that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus using the information listed below; the company you contact is required to notify the other two, which will place an alert on their versions of your credit report as well.

Equifax: 800 525-6285; www.equifax.com; P.O. Box 740231, Atlanta, GA 30374-0241

Experian: 888 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013;

TransUnion: 800 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you are entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your Social Security Number will appear on your credit reports. Carefully review any credit reports you receive. 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 and Social Security Number that is not accurate. If you see anything you do not understand, call the credit 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 information for law enforcement agency investigating the incident for the college/university]. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. You may also wish to file a complaint with the FTC at: www.consumer.gov/idtheft or 1877-ID-THEFT (438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Even if you do not find any signs of fraud on your reports, some consumer protection specialists recommend checking your credit report every three months for the next year. Just call one of the numbers listed above to order your reports and keep the fraud alert in place. For more information on identity theft, you may wish to review the resources available on the Minnesota Attorney General's Web site: www.ag.state.mn.us/consumer/Privacy/ or call the AGO Consumer Assistance Office at: 1-800 657-3787.

For all letters:

<College/university> regrets this incident and any inconvenience it may cause. If you have further questions related to this incident, please contact: <college/university contact>.