

Data Incident Notification Templates

If your school has a data incident, you will find the following collection of templates helpful. Included are the following:

- [Section One: Building a Press Release](#) page 2
- [Section Two: Notification Letter Components](#) page 6
- [Section Three: Incident Specific Website Template](#) page 8
- [Section Four: Incident Response FAQ](#) page 9
- [Section Five: Generic Identity Theft Web Site](#) page 11

The following table helps show the relationship of the five documents:

Table of Contents	Press Release	Notification Letter	Incident-specific Website Template	Incident Response FAQ	Generic Identity Theft Website Template
Introduction and Basic Description	yes	yes	yes		
Who is affected	yes	yes	yes	yes	
Incident Details	yes	yes	yes		
"Disclaimer"	yes	yes			
Apology or Statement of Commitment to Security	yes	yes			
Major (re) actions taken	yes	yes	yes		
For more information	yes	yes	yes		
Is my information stolen?				yes	
Still risk of disclosure?				yes	
If I discover fraudulent use?				yes	yes
Will I be contacted?				yes	
Who do I contact?				yes	yes
What is identity theft?					yes
How to protect yourself					yes
Steps if your data is stolen					yes
Credit Reporting Agencies					yes
Social Security Admin					yes
ID Theft Clearinghouse					yes
Law Enforcement					yes
Web Resources					yes

Section One: Building a Press Release

I. Elements of a press release

- a. What are you doing?
 - Announcing a breach? A theft?
 - Announcing that the case has been resolved? That notification has occurred?
- b. Who is affected/not affected? What specific types of personal information are involved?
- c. What are the (brief) details of the incident?
- d. "No evidence to indicate data has been misused..." or what the evidence points to.
- e. Expression of regret and concrete steps the institution is taking to prevent this from happening again.
- f. Major (re)actions taken.
- g. For more information, ...

II. Sample snippets

A. Introduction and Basic Description

1. University of Kansas officials today announced they have detected suspected computer hacking into a file server that contained records on 1,450 students, most of whom were international students.
2. University of California, Berkeley, police are investigating the theft of a campus laptop computer that contained files with the names and Social Security numbers of more than 98,000 individuals, mostly graduate students or applicants to the campus's graduate programs.
3. UCLA began mailing letters June 5 about the theft of a laptop computer from a locked van at a UCLA blood drive last November. The computer held a database containing personal information from some 145,000 people who have donated blood and platelets to the UCLA Blood and Platelet Center since 1985.
4. A Boston College student has been suspended from the University for violation of the University's computer use policy after he admitted to illegally obtaining personal identification numbers (PIN) and Social Security numbers of a number of BC students, staff, faculty and recent graduates by using keystroke-capturing software.

B. Who affected/personal information involved

5. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff.
6. The stolen computer contained information on most individuals who applied to graduate school at UC Berkeley between fall 2001 and spring 2004 (except law school students in the JD, LLM, and JSD programs); graduate students who registered at UC Berkeley between fall 1989 and fall 2003 (including law school students in the JD, LLM, and JSD programs); recipients of doctoral degrees from 1976 through 1999 (excluding law school students in the JD program); and other small groups of individuals. Approximately one-third of all of the computer's files contained dates of birth and/or addresses in addition to Social Security numbers and names.

7. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff. The vast majority of students involved were new students within the past five years. The faculty and staff data was contained in a file from the Wildcat Card identification system.
8. The server did not include any information related to the UConn Health Center's electronic patient records and no patient information was affected, said Kerntke.
9. Student laptop computers were not breached, and, at this time, school officials believe that [population e.g. current undergraduates] were not affected.

C. Incident details

10. Five apparent hacking incidents, which took place between Jan. 6 and 17, were discovered Jan. 21. Once officials determined yesterday that university data had been downloaded, the incidents were reported immediately to the Federal Bureau of Investigation, the INS and other appropriate agencies. The university is assisting the FBI in efforts to identify and apprehend the person or people responsible for the hacking.
11. The University discovered the hacking during routine monitoring of the network. An investigation revealed that the hackers installed software to store files, such as for movies or games, on the system and attempted to break into other computers.
12. The computer was stolen March 11 when an individual entered a restricted area of the Graduate Division offices that was momentarily unoccupied. A campus employee saw the individual leaving with the laptop and contacted campus police. The case remains under investigation.
13. According to Moore, an extensive computer forensics investigation concluded that the computer was not targeted to access personal information, but to allow the hacker to launch attacks on other computers on the Internet.
14. As a result of the detection, the computer was immediately taken off-line and the breach secured.

D. "Disclaimer"

15. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said. Kerntke advised individuals to consider submitting a fraud alert to the three national credit reporting agencies as this will make it more difficult for identity theft to occur.
16. "While this is worrisome, we have no evidence that anyone has extracted the private information and is using it," she added. "We wanted to advise our donors to be extra alert to signs of possible misuse of their personal identities."
17. In a statement to the media, Director of Public Affairs Jack Dunn said there was no evidence that personal information was accessed in any way, but given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database with Federal Trade Commission guidelines they could follow to help ensure their privacy.
18. "Based on forensic analysis, there is no indication that any of the data on the machine was actually compromised – only that the opportunity for someone to

access it existed," Kerntke said. "Even so, the University wants to be sure individuals are aware of the situation so they can carefully monitor their financial records for unauthorized activity over the next several months."

19. The student, whose identity is protected under student privacy laws, admitted to the dean of student development that he had gathered the information by exploiting a security hole in Microsoft Windows on several public computers on campus, but denied having divulged the information externally in any way. An investigation by the Boston College Police Department confirmed that the information was not misused externally.
20. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said.
21. No evidence of unauthorized use of personal information included on the computer system has been discovered. However, potential risks associated with identity theft are serious, and the school's administration has taken precautionary steps to inform all affected students, graduate alumni, faculty, staff and others whose information may have been contained on the system about safeguarding measures aimed at protecting privacy.
22. The University reports that it has no evidence that personal information was accessed in any way. However, given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database. The advisory includes FTC Guidelines to help guard against identity theft.

E. Apology or statement of commitment to security

23. "We deeply regret this situation and are taking steps to support the affected students," said Provost and Executive Vice Chancellor David Shulenburg. "We will help them in every way possible and do our best to protect against future intrusions."
24. "We deeply regret our delay and the security breach," she said. "We have put new measures into place to better assure that sensitive data stored on laptops are encrypted, protected and limited to essential need."
25. "Blood donors are generous people who sustain the lives of thousands of UCLA patients each year. We would feel terrible if any harm befell them," said Dr. Priscilla Figueroa, director of transfusion medicine for UCLA Medical Center.

F. Major (re)actions taken

26. "We are doing everything we can to prevent this from happening again in the future," he said, noting that the University is reviewing its dependence on social security numbers as a unique identifier, auditing other servers and departments that are not directly part of the breached system but contain or transmit sensitive information, and implementing even more stringent network and server access controls while striving to support the technologically collaborative environment essential to a comprehensive research institution like UConn.
27. Social Security numbers will display only the last 4 digits wherever possible. Helpdesk staff will assist UCLA Healthcare employees in removing private information from laptop and desktop computers and relocating it on secure network servers.

Employees must encrypt any sensitive information that needs to remain on their computer's local drive.

28. Upon learning of the breach, Executive Vice President Patrick J. Keating organized a task force of staff from Information Technology, Human Resources, Student Services, Student Affairs, BCPD and Public Affairs, along with a consultant from the Massachusetts State Police, to address the issue.

G. For more information

29. The School will provide updates for its constituents via the Internet. A Web site providing information and frequently asked questions can be found at [URL]. Affected individuals also can call 1-800 for more information or send an e-mail to school-incident@school.edu.
30. In addition, the University has established an alumni phone line at (866)683-6369 that will be staffed by BC employees to answer questions regarding the breach. Information is also available at www.bc.edu/offices/techsupport/security/
31. Keating suggested that any faculty and staff with questions on this issue should contact the Office of Human Resources at ext.2-3330. Students should contact Student Services at ext.2-8900.

Section Two: Notification Letter Components

Edit the following components into a letter of notification or web site statement. Headings are boldface, several examples follow each heading. Delete the heading; edit the sample text into your letter.

Disclaimers: Don't disclose anything that hampers the investigation, gives additional information to those who would do harm, etc. Consult your university legal counsel. Release information only through university approved channels.

What happened?

(E.g., a server/laptop/desktop was breached/stolen/lost in <school or location>)

Example: In December 2004, campus officials were notified of the theft of an [department name] laptop computer

Example: . . . an on-campus server containing data on University international students was a target of computer hacking. As a result, these data were downloaded from the machine.

When did the breach occur and/or when was it detected?

Example: In December 2004, campus officials were notified . . .

Example: Late yesterday, the University discovered that on February 29, 2004 ...

How was it detected?

What data was potentially compromised?

Example: This computer contained a list of [department] student employees. The list included the names and Social Security Numbers of the students.

Example: The data fields downloaded were: name, telephone number, University email address (if one was registered), social security number, date of birth, University identification number, passport number, city and country of birth, country of citizenship, school and department, degree sought, major field, University employee identification number (if employed at the University), non-immigration classification (e.g., F-1, J-1, etc.), and local and permanent address. Not all of these fields were filled for every student. It is also probable that a small number of students included in the database were domestic students who had been identified as international students prior to verification.

How much data was compromised?

Example: Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data . . .

For whom was data compromised?

Why you are being notified.

Example: The file downloaded during this theft may have contained some information about you.

Example: We are notifying you of this security breach because you are one of the students whose personal information was present on the laptop. Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data, we are bringing this incident to your attention, in accordance with California law, so that you can be extra alert to signs of any possible misuse of your personal identity.

What steps are/were being taken?

(e.g. machine taken off the net, law enforcement (local/FBI), Credit card companies notified (for cases where contact information is needed about cardholders), etc)

Example: The server was originally secure but became vulnerable when a Microsoft security update to the operating system was installed. Security to the system has since been restored.

Several offices at the University, including Information Services and the Provost, are working hard to address problems caused by this incident and any further implications it might have for you. As the situation develops, we will send additional messages regarding further actions or precautions that you should take.

Is any data known to be fraudulently used or is notification precautionary?

What steps should individuals take?

(E.g., place a fraud alert with the credit bureaus, contact credit card companies, close accounts, etc.)

Example: Please monitor your email in the coming days for messages from The University.

Example: Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps you can take, exercising abundant caution, to protect yourself. First, you may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency. The following references provide additional information about identity theft:

- Federal Trade Commission website on identity theft (<http://www.consumer.gov/idtheft/>)
- Social Security Administration fraud line at 1-800-269-0271
- Major Credit Bureau Numbers
 - Equifax 1-800-525-6285
 - Experian 1-888-397-3742
 - Trans Union 1-800-680-7289
- Identity Theft Victim Checklist (<http://www.privacy.ca.gov/sheets/cis3english.pdf>)

Apology or statement of commitment to security

Example: We deeply regret this situation and any inconvenience or alarm it may cause you.

Example: We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The University is committed to maintaining the privacy of student information and takes many precautions for the security of personal information. In response to incidents of theft like this one and the increasing number of internet-enabled computer attacks, the University is

continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

Anticipated next steps, if any.

E.g., intention to notify if any additional information becomes available?

Example: The theft of this information raises a number of possible risks to you. One is theft of identity for financial gain. The University will be sending you a package of materials outlining steps you can take to protect yourself from this. Another risk is theft of identity for purposes of international travel or foreign entry. The University is currently working with several federal agencies, including the Immigration and Naturalization Service, and we have been informed that because of this theft, you may be asked further questions to verify your identity when leaving or entering the United States.

Who to contact for additional information

Contact/name, number, hours of availability, web site, hotline, email address, etc.

Example: Should you have further questions about this matter, please contact [name of contact], [title of contact], at [email address of contact] or [phone number].

Signature

Who makes most sense – president, dean, other contact familiar to the individual, consider multiple signatories for different constituent groups.

Section Three: Incident Specific Website Template

Common elements:

Most-Recent-Update section at top of page

Basic facts (similar to what might appear in a notification letter):

- Who was impacted
- What data may have been involved
- When compromise or discovery occurred
- Where compromise occurred
- Whether anyone believed to be negatively affected or not

Actions taken by unit/University to ensure more secure in future/Ongoing measures

What should I do to be sure I'm unaffected?

Link to Identity Theft website/credit agencies

FAQs

Press Releases

Toll-free Hotline contact information

Where site hosted/located:

On Public Safety site

On compromised unit's site

On a specially dedicated "datatheft" website: www.univname.edu/datatheft
(This places all data-related incidents in one place in chronological order; provides community members an easy-to-regularly-check place to look to see if they're affected.)

Section Four: Incident Response FAQ

This template can be used to guide development of “frequently asked questions” information to include as part of a notification letter, website or other materials concerning a specific security incident. Answers to questions in this template are examples only. They need to be adjusted for the unique circumstances of the incident.

Individuals potentially affected by an incident will have varying levels of computing knowledge – possibly none. It is, therefore, critical that explanations of the incident, the potential for impact on them, and steps they should take, if any, be communicated in clear and concise terms. Institutions should carefully consider the specific information these individuals will want to know and address only those issues. Explanations should be short, to the point, and free of technical jargon.

Question. I received a notification via e-mail/letter from (institution name) about a computer security incident. Does that mean someone stole my personal information?

Example Answer. No. The (institution name)’s investigation into this incident revealed that an unauthorized person gained control of a computer containing a confidential file. It is possible the intruder’s intent was to either disrupt normal business or use the computer’s processing power to launch similar attacks on other computers. He or she may not have been aware the confidential file was stored on this computer. We do not have sufficient evidence, however, that the file was not acquired. The (institution name) has, therefore, taken the precautionary measure of distributing an advisory to all individuals whose information was in the file, so that they can take appropriate steps if concerned. Thus far, there have been no reports of unauthorized use of personal information as a result of this computer security breach.

Question. What personal information was involved? When was it available to the unauthorized person?

Example Answer. The confidential file contained names, addresses, birth dates, and social security numbers of individuals who submitted applications for admission to the (institution name/school) in 2004. Current information indicates the unauthorized person gained control of the computer from September 1, 2005 to September 8, 2005.

Question. Is this information still at risk of disclosure to an unauthorized person?

Example Answer. The computer involved in this incident has been secured. The (institution name) is taking precautions to minimize future security risks.

Question. What should I do if I discover fraudulent use of my personal information?

Example Answer. Individuals whose personal information was involved in this incident can request a free initial fraud alert to be placed on their credit files by calling any one of the three major national credit bureaus:

- **Equifax**
Direct Line for reporting suspected fraud:
800-525-6285
 Fraud Division
 P.O. Box 740250
 Atlanta, GA 30374
 800-685-1111 / 888-766-0008
<http://www.equifax.com>

- **Experian**
Direct Line for reporting suspected fraud:
888-397-3742
 Credit Fraud Center
 P.O. Box 1017
 Allen, TX 75013
 888-EXPERIAN (888-397-3742)
<http://www.experian.com>

- **Trans Union**
Direct Line for reporting suspected fraud:
800-680-7289
 Fraud Victim Assistance Department
 P.O. Box 6790
 Fullerton, CA 92634
 Phone: 800-916-8800 / 800-680-7289
<http://www.transunion.com>

When contacting the Credit Reporting Agency, you should request the following:

1. Instruct them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.
2. Ask them for copies of your credit report(s). **(Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.)**
 Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts.
NOTE: In order to ensure that you are issued free credit reports, we strongly encourage you to contact the agencies **DIRECT LINE (listed above) for reporting fraud.** We do not recommend that you order your credit report online.
3. Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
4. If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission to help make your case with creditors.

Question. Will (institution name) contact me to ask for private information because of this event?

Example Answer. In similar cases at other institutions, people have reportedly been contacted by individuals claiming to represent the University and who then proceed to ask for personal information, including social security numbers and/or credit card information. Please be aware that (institution name) will only contact you about this incident if additional helpful information becomes available. We will not ask for your full Social Security number. We will not ask for credit card or bank information. We recommend that you do not release personal information in response to any contacts of this nature that you have not initiated.

Question. Who should I contact if I have any additional questions concerning this security breach?

Example Answer. In order to answer any questions that you may have regarding this incident a special phone line, (xxx) xxx-xxxx (toll free 1-888-xxx-xxxx), has been activated and will be monitored by the (institution's name).

Section Five: Generic Identity Theft Web Site

Generic Identity Theft Web Site Template

Instructions: Use this template to create a generic identity theft website to be perpetually published as a public service announcement to your institution's community. It can subsequently be linked from any incident specific site.

Make sure to verify that contact information is correct at the time you publish and review all content for application to your institution and location.

There are many excellent resources and sources whose primary purpose is to educate the community at large about identity theft and preventive measures. The following template pulls from those sources and from the public websites of many institutions of higher education. The template includes information about the most important aspects of the topic like what it is, how to protect yourself, and what to do if you become a victim but omits other aspects that are covered by the resources linked in the resources section like how does it most frequently occur and what are the most common crimes committed. Thus the generic site template does not attempt to recreate all of the available information; rather, it provides a general overview.

Template:

Introduction

This site contains information on how to protect yourself from identity theft as well as what to do to if your personal information becomes exposed or if you actually become a victim of identity theft. Links to additional information can be found under the Resources.

What is Identity Theft?

Identity theft occurs when someone uses another person's personal information such as name, Social Security number, driver's license number, credit card number or other identifying information to take on that person's identity in order to commit fraud or other crimes.

How to Protect Yourself from Identity Theft

The following tips can help lower your risk of becoming a victim of identity theft.

1. **Protect your Social Security number.** Don't carry your Social Security card or other cards that show your SSN. Read, "Your Social Security Number: Controlling the Key to Identity Theft" (http://www.ssa.gov/oig/executive_operations/factsheet1.htm)
2. **Use caution when giving out your personal information.** Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in postal mail.

3. **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.
4. **Protect your postal mail.** Retrieve mail promptly. Discontinue delivery while out of town.
5. **Check your bills and bank statements.** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
6. **Check your credit reports.** Review your credit report at least once a year. Check for changed addresses and fraudulent charges.
7. **Stop pre-approved credit offers.** Pre-approved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. **Call toll-free 888-5OPTOUT (888-567-8688).**
8. **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give your personal information.
9. **Protect your computer.** Protect personal information on your computer by following good security practices.
 - Use strong, non-easily guessed passwords.
 - Use firewall, anti-virus, and anti-spyware software that you update regularly.
 - Download software only from sites you know and trust and only after reading all the terms and conditions.
 - Don't click on links in pop-up windows or in spam e-mail.
10. **Use caution on the Web.** When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell if a page is secure if "**https**" is in URL or if there is a padlock icon on the browser window.

Steps to Take if Your Data Becomes Compromised or Stolen

Credit Reporting Agencies

If you have reason to believe your personal information has been compromised or stolen, contact the Fraud Department of one of the three major credit bureaus listed below.

- [**Equifax**](#)
Direct Line for reporting suspected fraud:
800-525-6285
Fraud Division
P.O. Box 740250

Atlanta, GA 30374
800-685-1111 / 888-766-0008
<http://www.equifax.com>

- **Experian**
Direct Line for reporting suspected fraud:
888-397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
888-EXPERIAN (888-397-3742)
<http://www.experian.com>
- **Trans Union**
Direct Line for reporting suspected fraud:
800-680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
Phone: 800-916-8800 / 800-680-7289
<http://www.transunion.com>

When contacting the Credit Reporting Agency, you should request the following:

5. Instruct them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.
6. Ask them for copies of your credit report(s). **(Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.)** Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. **NOTE:** In order to ensure that you are issued free credit reports, we strongly encourage you to contact the agencies **DIRECT LINE (listed above) for reporting fraud.** We do not recommend that you order your credit report online.
7. Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
8. If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission to help make your case with creditors.

Social Security Administration
SSA Fraud Hotline: 800-269-0271
<http://www.ssa.gov/>

If you are the victim of a stolen Social Security number, the SSA can provide information on how to report the fraudulent use of your number and how to correct your earnings record.

We encourage you to contact the **Fraud Hotline** immediately once you suspect identity theft.

The website also provides tips on using and securing your Social Security number. Visit the SSA website for advice on [keeping your number safe](#).

ID Theft Clearinghouse

1-877-ID-THEFT (1-877-438-4338)

Call the ID Theft Clearinghouse toll free at to report identity theft. Counselors will take your complaint and advise you how to deal with the credit-related problems that could result from identity theft.

Local Law Enforcement

It is important that you report identity theft to your local police department as soon as you become aware that you are a victim. Get a copy of the police report which will assist you when notifying creditors, credit reporting agencies and if necessary, the Social Security Administration (SSA).

Resources

The following links provide detailed information related to identity theft and protecting yourself.

Department of Justice

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

Federal Trade Commission

<http://www.consumer.gov/idtheft/>

Social Security Administration

http://www.ssa.gov/oig/executive_operations/factsheet1.htm

Privacy Rights Clearinghouse - Identity Theft Resources

<http://www.privacyrights.org/identity.htm>

National Fraud Information Center Hotline: 800-876-7060

Identity Theft Resource Center: 858-693-7935

Contact Us

Create email link.

NEXT SECTION IS SAME INFO AS PREVIOUS, BUT SEGMENTED IN A DIFFERENT WAY TO SUPPORT THE FIRST COLUMN OF HYPERLINKS

Introduction and Basic Description

32. (E.g. A server/laptop/desktop was breached/stolen/lost in <school or location>)
33. Example: In December 2004, campus officials were notified of the theft of an [department name] laptop computer
34. Example: . . . an on-campus server containing data on University international students was a target of computer hacking. As a result, these data were downloaded from the machine
35. University of Kansas officials today announced they have detected suspected computer hacking into a file server that contained records on 1,450 students, most of whom were international students.
36. University of California, Berkeley, police are investigating the theft of a campus laptop computer that contained files with the names and Social Security numbers of more than 98,000 individuals, mostly graduate students or applicants to the campus's graduate programs.
37. UCLA began mailing letters June 5 about the theft of a laptop computer from a locked van at a UCLA blood drive last November. The computer held a database containing personal information from some 145,000 people who have donated blood and platelets to the UCLA Blood and Platelet Center since 1985.
38. A Boston College student has been suspended from the University for violation of the University's computer use policy after he admitted to illegally obtaining personal identification numbers (PIN) and Social Security numbers of a number of BC students, staff, faculty and recent graduates by using keystroke-capturing software.

Who is affected?

39. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff.
40. The stolen computer contained information on most individuals who applied to graduate school at UC Berkeley between fall 2001 and spring 2004 (except law school students in the JD, LLM, and JSD programs); graduate students who registered at UC Berkeley between fall 1989 and fall 2003 (including law school students in the JD, LLM, and JSD programs); recipients of doctoral degrees from 1976 through 1999 (excluding law school students in the JD program); and other small groups of individuals. Approximately one-third of all of the computer's files contained dates of birth and/or addresses in addition to Social Security numbers and names.
41. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff. The vast majority of students involved were new students within the past five years. The faculty and staff data was contained in a file from the Wildcat Card identification system.
42. The server did not include any information related to the UConn Health Center's electronic patient records and no patient information was affected, said Kerntke.
43. Student laptop computers were not breached, and, at this time, school officials believe that [population e.g. current undergraduates] were not affected.
44. The confidential file contained names, addresses, birth dates, and social security numbers of individuals who submitted applications for admission to the (institution name/school) in 2004.

Incident Details

45. Five apparent hacking incidents, which took place between Jan. 6 and 17, were discovered Jan. 21. Once officials determined yesterday that university data had been downloaded, the incidents were reported immediately to the Federal Bureau of Investigation, the INS and other appropriate agencies. The university is assisting the FBI in efforts to identify and apprehend the person or people responsible for the hacking.
46. The University discovered the hacking during routine monitoring of the network. An investigation revealed that the hackers installed software to store files, such as for movies or games, on the system and attempted to break into other computers.
47. The computer was stolen March 11 when an individual entered a restricted area of the Graduate Division offices that was momentarily unoccupied. A campus employee saw the individual leaving with the laptop and contacted campus police. The case remains under investigation.
48. According to Moore, an extensive computer forensics investigation concluded that the computer was not targeted to access personal information, but to allow the hacker to launch attacks on other computers on the Internet.
49. As a result of the detection, the computer was immediately taken off-line and the breach secured.
50. **What happened?**

(E.g. A server/laptop/desktop was breached/stolen/lost in <school or location>)

Example: In December 2004, campus officials were notified of the theft of an [department name] laptop computer

Example: . . . an on-campus server containing data on University international students was a target of computer hacking. As a result, these data were downloaded from the machine.

When did the breach occur and/or when was it detected?

Example: In December 2004, campus officials were notified . . .

Example: Late yesterday, the University discovered that on February 29, 2004 ...

How was it detected?

What data was potentially compromised?

Example: This computer contained a list of [department] student employees. The list included the names and Social Security Numbers of the students.

Example: The data fields downloaded were: name, telephone number, University email address (if one was registered), social security number, date of birth, University identification number, passport number, city and country of birth, country of citizenship, school and department, degree sought, major field, University employee identification number (if employed at the University), non-immigration classification (e.g., F-1, J-1, etc.), and local and permanent address. Not all of these fields were filled for every student. It is also probable that a small number of

students included in the database were domestic students who had been identified as international students prior to verification.

How much data was compromised?

Example: Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data . . .

For whom was data compromised?

Disclaimer

Don't disclose anything that hampers the investigation, gives additional information to those who would do harm, etc. Consult your university legal counsel. Release information only through university approved channels.

51. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said. Kerntke advised individuals to consider submitting a fraud alert to the three national credit reporting agencies as this will make it more difficult for identity theft to occur.
52. "While this is worrisome, we have no evidence that anyone has extracted the private information and is using it," she added. "We wanted to advise our donors to be extra alert to signs of possible misuse of their personal identities."
53. In a statement to the media, Director of Public Affairs Jack Dunn said there was no evidence that personal information was accessed in any way, but given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database with Federal Trade Commission guidelines they could follow to help ensure their privacy.
54. "Based on forensic analysis, there is no indication that any of the data on the machine was actually compromised – only that the opportunity for someone to access it existed," Kerntke said. "Even so, the University wants to be sure individuals are aware of the situation so they can carefully monitor their financial records for unauthorized activity over the next several months."
55. The student, whose identity is protected under student privacy laws, admitted to the dean of student development that he had gathered the information by exploiting a security hole in Microsoft Windows on several public computers on campus, but denied having divulged the information externally in any way. An investigation by the Boston College Police Department confirmed that the information was not misused externally.
56. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said.
57. No evidence of unauthorized use of personal information included on the computer system has been discovered. However, potential risks associated with identity theft are serious, and the school's administration has taken precautionary steps to inform all affected students, graduate alumni, faculty, staff and others whose information may have been contained on the system about safeguarding measures aimed at protecting privacy.
58. The University reports that it has no evidence that personal information was accessed in any way. However, given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database. The advisory includes FTC Guidelines to help guard against identity theft.

Apology or Statement of Commitment to Security

59. "We deeply regret this situation and are taking steps to support the affected students," said Provost and Executive Vice Chancellor David Shulenburger. "We will help them in every way possible and do our best to protect against future intrusions."
60. "We deeply regret our delay and the security breach," she said. "We have put new measures into place to better assure that sensitive data stored on laptops are encrypted, protected and limited to essential need."
61. "Blood donors are generous people who sustain the lives of thousands of UCLA patients each year. We would feel terrible if any harm befell them," said Dr. Priscilla Figueroa, director of transfusion medicine for UCLA Medical Center.
62. Example: We deeply regret this situation and any inconvenience or alarm it may cause you.
63. Example: We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The University is committed to maintaining the privacy of student information and takes many precautions for the security of personal information. In response to incidents of theft like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

Major (re)actions taken

64. "We are doing everything we can to prevent this from happening again in the future," he said, noting that the University is reviewing its dependence on social security numbers as a unique identifier, auditing other servers and departments that are not directly part of the breached system but contain or transmit sensitive information, and implementing even more stringent network and server access controls while striving to support the technologically collaborative environment essential to a comprehensive research institution like UConn.
65. Social Security numbers will display only the last 4 digits wherever possible. Helpdesk staff will assist UCLA Healthcare employees in removing private information from laptop and desktop computers and relocating it on secure network servers. Employees must encrypt any sensitive information that needs to remain on their computer's local drive.
66. Upon learning of the breach, Executive Vice President Patrick J. Keating organized a task force of staff from Information Technology, Human Resources, Student Services, Student Affairs, BCPD and Public Affairs, along with a consultant from the Massachusetts State Police, to address the issue.
67. (e.g. machine taken off the net, law enforcement (local/FBI), Credit card companies notified (for cases where contact information is needed about cardholders), etc)
68. Example: The server was originally secure but became vulnerable when a Microsoft security update to the operating system was installed. Security to the system has since been restored.
69. Several offices at the University, including Information Services and the Provost, are working hard to address problems caused by this incident and any further implications it might have for you. As the situation develops, we will send additional messages regarding further actions or precautions that you should take.

For more information

70. The School will provide updates for its constituents via the Internet. A Web site providing information and frequently asked questions can be found at [URL]. Affected individuals also can call 1-800 for more information or send an e-mail to school-incident@school.edu.
71. In addition, the University has established an alumni phone line at (866)683-6369 that will be staffed by BC employees to answer questions regarding the breach. Information is also available at www.bc.edu/offices/techsupport/security/
72. Keating suggested that any faculty and staff with questions on this issue should contact the Office of Human Resources at ext.2-3330. Students should contact Student Services at ext.2-8900.
73. Contact/name, number, hours of availability, web site, hotline, email address, etc.
74. Example: Should you have further questions about this matter, please contact [name of contact], [title of contact], at [email address of contact] or [phone number].

Is my information stolen?

Example Answer. No. The (institution name)'s investigation into this incident revealed that an unauthorized person gained control of a computer containing a confidential file. It is possible the intruder's intent was to either disrupt normal business or use the computer's processing power to launch similar attacks on other computers. He or she may not have been aware the confidential file was stored on this computer. We do not have sufficient evidence, however, that the file was not acquired. The (institution name) has, therefore, taken the precautionary measure of distributing an advisory to all individuals whose information was in the file, so that they can take appropriate steps if concerned. Thus far, there have been no reports of unauthorized use of personal information as a result of this computer security breach.

Still risk of disclosure?

Example Answer. The computer involved in this incident has been secured. The (institution name) is taking precautions to minimize future security risks.

What should I do if I discover fraudulent use of my personal information?

Example Answer. Individuals whose personal information was involved in this incident can request a free initial fraud alert to be placed on their credit files by calling any one of the three major national credit bureaus:

- **[Equifax](#)**
Direct Line for reporting suspected fraud:
800-525-6285
Fraud Division
P.O. Box 740250
Atlanta, GA 30374
800-685-1111 / 888-766-0008
<http://www.equifax.com>
- **[Experian](#)**
Direct Line for reporting suspected fraud:
888-397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
888-EXPERIAN (888-397-3742)
<http://www.experian.com>
- **[Trans Union](#)**
Direct Line for reporting suspected fraud:
800-680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
Phone: 800-916-8800 / 800-680-7289
<http://www.transunion.com>

When contacting the Credit Reporting Agency, you should request the following:

9. Instruct them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.
10. Ask them for copies of your credit report(s). **(Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.)**
Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts.
NOTE: In order to ensure that you are issued free credit reports, we strongly encourage you to contact the agencies **DIRECT LINE (listed above) for reporting fraud.** We do not recommend that you order your credit report online.
11. Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
12. If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission to help make your case with creditors.

Will I be contacted?

Example Answer. In similar cases at other institutions, people have reportedly been contacted by individuals claiming to represent the University and who then proceed to ask for personal information, including social security numbers and/or credit card information. Please be aware that (institution name) will only contact you about this incident if additional helpful information becomes available. We will not ask for your full Social Security number. We will not ask for credit card or bank information. We recommend that you do not release personal information in response to any contacts of this nature that you have not initiated.

Who do I contact?

Example Answer. In order to answer any questions that you may have regarding this incident a special phone line, (xxx) xxx-xxxx (toll free 1-888-xxx-xxxx), has been activated and will be monitored by the (institution's name).