



Children's Hospital Boston

A teaching affiliate of Harvard Medical School

300 Longwood Avenue, Boston, Massachusetts 02115
617-355-6000
www.childrenshospital.org

January 12, 2009

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Coakley:

Pursuant to M.G.L. c. 93H, I am writing to notify you of a possible unauthorized access or use of personal information involving 31 Massachusetts residents.

On November 12, 2008, one of our employees reported a laptop stolen from a clinical office area. The laptop was not encrypted. Initially, a determination was made that no personal information was saved to the laptop. However, during the course of our review, it was discovered that any information that is viewed on the laptop, such as email, may be accessible in the laptop's "cache" even though the information was not saved. Our Information Security staff used a new tool to search through the email files of the employee who used the laptop to review her email in order to more accurately determine whether there was personal information in her email files that would likely have been stored in the laptop's cache. Our review using this new tool has uncovered several email records that contained a name along with either a social security number, insurance subscriber number, or both. These records affect 31 Massachusetts residents and 120 other individuals, for many of whom we have no residence information. More specifically, the information we believe may have been in the laptop cache includes:

1. A spreadsheet containing names, dates of birth and SSNs for 114 Cirque de Soleil employees. The laptop was used by our Sports Medicine group, which contracts with organizations (including Cirque de Soleil) to provide medical coverage for performance and sporting events. Although we do not ask for personal information about event participants in these circumstances, the company sent the spreadsheet so that if one of those performers required medical attention at or immediately after the event, registration of the performer as a patient would be expedited. Nearly all of the individuals received no services, and the information in the spreadsheet was not used. Even the few who did receive services listed Cirque de Soleil, based in Las Vegas, NV, as their residence.
2. Thirty-nine pre-registration forms sent by area organizations that refer patients to the Sports Medicine group. These forms include name and insurance subscriber number; 18 of them also include a social security number. Of these, ten of the records

including SSN and five of the records including only the insurance number (i.e., 15 total) affect Massachusetts residents.

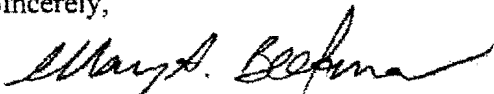
7. A list of 16 Children's providers, all Massachusetts residents, that includes names, various billing numbers, and social security numbers. The list was circulated to internal administrative staff by email and was used for billing purposes.

Upon receiving notice of the theft, our Facility Security and Information Security staff undertook an investigation. A police report was filed with the Boston Police Department. We have no indication or evidence that any fraud has been committed or that this personal information has been either retrieved or misused. We intend to offer 2 years of credit monitoring services to individuals whose social security number was involved. In addition, we have worked with the department to ensure that all of its remaining laptops are encrypted, as required under existing Hospital policy, and are issuing reminder notices to other departments about the policy. The department has also (1) adopted a policy of not accepting or immediately deleting Social Security numbers received from event organizers; (2) made outreach to the groups and organizations with which it maintains ongoing relationships to request that no social security numbers be sent; (4) established an alternative method of sharing provider billing information internally with staff and ensuring that all copies of the provider listing that included SSNs are destroyed. Finally, we will be providing reinforcement training for the department to reinforce data security policies and ensure that staff understand the risks and requirements around data security, including the importance of adhering to the institution's laptop encryption policy.

We have provided a similar notice to the Director of Consumer Affairs and Business Regulation. We plan to notify Cirque de Soleil about the incident and will work with the company to coordinate notification to its employees about the incident and the availability of credit monitoring. We will also provide written notice to the other affected individuals. A copy of the letter we will use to notify Massachusetts residents is attached.

Please contact me if you have any questions or concerns or need further information.

Sincerely,



Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Draft Letter to Mass. Resident (Name and SSN specific) w/ offer of Credit Report monitoring services

Date

Name

Address

City/Town/State and Zip

Dear :

I am writing to notify you about a possible unauthorized access to or use of your personal information that occurred on or about November 11, 2008, and was identified in late December 2008. We have no indication or evidence that any fraud has been committed or that your personal information has either been retrieved or misused. However, out of an abundance of caution, we wanted to notify you so that you may properly evaluate what actions you may want to consider taking to minimize any potential risks and to protect yourself, as well as what action we plan to take on your behalf. We recommend that you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution.

Under Massachusetts law, you have the right to obtain any police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit report. A security freeze prohibits a credit reporting agency from releasing any information about a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788

Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Found Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or compliant to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit monitoring agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and social security number) **and** the PIN number or password provided to you when you placed the security

freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

In addition, you may place a "fraud alert" on your credit file by contacting the fraud department of any one of the three major credit bureaus. The fraud alert requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three credit bureaus are required by law to automatically send a credit report free of charge to you. This "one-call" fraud alert will remain in your credit file for at least 90 days. When you receive your credit reports, review them carefully for any unexplained activity.

We recommend that you review your credit card and other financial account information regularly for any suspicious or unauthorized activity. *[To help you detect possible misuse of your personal information, we are providing you with a complimentary 2-year membership in Experian's Triple Alert credit monitoring service at no cost to you. This will allow for your credit reports to be monitored at the three national credit reporting companies (Experian, Equifax and TransUnion) and for you to be notified of key changes. You have ninety (90) days to activate this membership, which will then continue for 24 full months. Enrollment in this program will not hurt your credit score. We encourage you to activate your credit monitoring membership as soon as possible.*

The website to enroll in Triple Alert and your individual activation code are both listed below. To sign up, please visit the website and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The website will guide you through the process of enrolling in Triple Alert. If you need technical assistance, please call [insert Experian number].

Triple Alert Website: [insert URL]

Your Activation Code: [insert activation code]

If you wish to enroll over the phone for delivery of your membership via US Mail, please call 8xx-xxx-xxxx.]

Please accept our sincere apologies for this incident. We are committed to protecting confidential and personal information and have taken steps to avoid having this kind of incident happen again. Please contact me if you have any questions about this incident or need further information.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Note: Italicized text will appear only in letters to individuals whose social security number is involved.

Draft Written Notification to Cirque De Soleil, 1_9_09

Date

Address

Dear :

I am writing in follow-up to our earlier conversation to provide you with written notice of an incident in which personal information of 114 of your employees may have been subject to unauthorized acquisition or use. On November 12, 2008, one of the employees in our Sports Medicine department reported a laptop stolen from a clinical office area. The laptop was not encrypted. Initially, a determination was made that no personal information was saved to the laptop. However, during the course of our review, it was discovered that any information that is viewed on the laptop, such as email, may be accessible in the laptop's "cache" even though the information was not saved. Our Information Security staff used a new tool to search through the email files of the employee who used the laptop to review her email in order to more accurately determine whether there was personal information in her email files that would likely have been stored in the laptop's cache. Our review using this new tool has uncovered several email records that contained personal information, including a spreadsheet sent to the Sports Medicine group by Cirque de Soleil that included the name, date of birth, and Social Security Number of 114 of your employees. Although we did not require or request that this personal information be provided, the list was reportedly sent so that if one of those employees required medical attention at or immediately after the event being monitored by our Sports Medicine clinicians, registration of the performer as a patient would be expedited. Nearly all of these individuals did not receive any services from Children's and we have no further information, such as their mailing address. Even the approximately ten individuals who did receive services did not provide their residence address, and instead listed the company's place of business (in Las Vegas, Nevada) as their residence.

We have no indication or evidence that any fraud has been committed or that any of this personal information has been either retrieved or misused. We intend to offer 2 years of credit monitoring services to individuals whose social security number was involved. To facilitate the extension of this offer to the 114 Cirque de Soleil individuals, we are enclosing a model letter of notification with instructions on how to enroll in the program.

We will work with you to coordinate the specific enrollment information to be included in each letter.

We have worked with the department to ensure that all of its remaining laptops are encrypted, as required under existing Hospital policy, and are issuing reminder notices to other departments about the policy. The department has also (1) adopted a policy of not accepting or immediately deleting Social Security numbers received from event organizers; (2) made outreach to the groups and organizations with which it maintains ongoing relationships to request that no social security numbers be sent; (4) established an alternative method of sharing provider billing information internally with staff and ensuring that all copies of the provider listing that included SSNs are destroyed. Finally, we will be providing reinforcement training for the department to reinforce data security policies and ensure that staff understand the risks and requirements around data security, including the importance of adhering to the institution's laptop encryption policy.

Please contact me if you have any questions or concerns, and to discuss logistics of generating the individual notification letters.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Date

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Coakley:

Pursuant to M.G.L. c. 93H, I am writing to notify you of a possible unauthorized access or use of personal information involving 31 Massachusetts residents.

On November 12, 2008, one of our employees reported a laptop stolen from a clinical office area. The laptop was not encrypted. Initially, a determination was made that no personal information was saved to the laptop. However, during the course of our review, it was discovered that any information that is viewed on the laptop, such as email, may be accessible in the laptop's "cache" even though the information was not saved. Our Information Security staff used a new tool to search through the email files of the employee who used the laptop to review her email in order to more accurately determine whether there was personal information in her email files that would likely have been stored in the laptop's cache. Our review using this new tool has uncovered several email records that contained a name along with either a social security number, insurance subscriber number, or both. These records affect 31 Massachusetts residents and 120 other individuals, for many of whom we have no residence information. More specifically, the information we believe may have been in the laptop cache includes:

1. A spreadsheet containing names, dates of birth and SSNs for 114 Cirque de Soleil employees. The laptop was used by our Sports Medicine group, which contracts with organizations (including Cirque de Soleil) to provide medical coverage for performance and sporting events. Although we do not ask for personal information about event participants in these circumstances, the company sent the spreadsheet so that if one of those performers required medical attention at or immediately after the event, registration of the performer as a patient would be expedited. Nearly all of the individuals received no services, and the information in the spreadsheet was not used. Even the few who did receive services listed Cirque de Soleil, based in Las Vegas, NV, as their residence.
2. Thirty-nine pre-registration forms sent by area organizations that refer patients to the Sports Medicine group. These forms include name and insurance subscriber number; 18 of them also include a social security number. Of these, ten of the records including SSN and five of the records including only the insurance number (i.e., 15 total) affect Massachusetts residents.

3. A list of 16 Children's providers, all Massachusetts residents, that includes names, various billing numbers, and social security numbers. The list was circulated to internal administrative staff by email and was used for billing purposes.

Upon receiving notice of the theft, our Facility Security and Information Security staff undertook an investigation. A police report was filed with the Boston Police Department. We have no indication or evidence that any fraud has been committed or that this personal information has been either retrieved or misused. We intend to offer 2 years of credit monitoring services to individuals whose social security number was involved. In addition, we have worked with the department to ensure that all of its remaining laptops are encrypted, as required under existing Hospital policy, and are issuing reminder notices to other departments about the policy. The department has also (1) adopted a policy of not accepting or immediately deleting Social Security numbers received from event organizers; (2) made outreach to the groups and organizations with which it maintains ongoing relationships to request that no social security numbers be sent; (4) established an alternative method of sharing provider billing information internally with staff and ensuring that all copies of the provider listing that included SSNs are destroyed. Finally, we will be providing reinforcement training for the department to reinforce data security policies and ensure that staff understand the risks and requirements around data security, including the importance of adhering to the institution's laptop encryption policy.

We have provided a similar notice to the Director of Consumer Affairs and Business Regulation. We plan to notify Cirque de Soleil about the incident and will work with the company to coordinate notification to its employees about the incident and the availability of credit monitoring. We will also provide written notice to the other affected individuals. A copy of the letter we will use to notify Massachusetts residents is attached.

Please contact me if you have any questions or concerns or need further information.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Draft Written Notification to Cirque De Soleil, 1_9_09

Date

Address

Dear :

I am writing in follow-up to our earlier conversation to provide you with written notice of an incident in which personal information of 114 of your employees may have been subject to unauthorized acquisition or use. On November 12, 2008, one of the employees in our Sports Medicine department reported a laptop stolen from a clinical office area. The laptop was not encrypted. Initially, a determination was made that no personal information was saved to the laptop. However, during the course of our review, it was discovered that any information that is viewed on the laptop, such as email, may be accessible in the laptop's "cache" even though the information was not saved. Our Information Security staff used a new tool to search through the email files of the employee who used the laptop to review her email in order to more accurately determine whether there was personal information in her email files that would likely have been stored in the laptop's cache. Our review using this new tool has uncovered several email records that contained personal information, including a spreadsheet sent to the Sports Medicine group by Cirque de Soleil that included the name, date of birth, and Social Security Number of 114 of your employees. Although we did not require or request that this personal information be provided, the list was reportedly sent so that if one of those employees required medical attention at or immediately after the event being monitored by our Sports Medicine clinicians, registration of the performer as a patient would be expedited. Nearly all of these individuals did not receive any services from Children's and we have no further information, such as their mailing address. Even the approximately ten individuals who did receive services did not provide their residence address, and instead listed the company's place of business (in Las Vegas, Nevada) as their residence.

We have no indication or evidence that any fraud has been committed or that any of this personal information has been either retrieved or misused. We intend to offer 2 years of credit monitoring services to individuals whose social security number was involved. To facilitate the extension of this offer to the 114 Cirque de Soleil individuals, we are enclosing a model letter of notification with instructions on how to enroll in the program.

We will work with you to coordinate the specific enrollment information to be included in each letter.

We have worked with the department to ensure that all of its remaining laptops are encrypted, as required under existing Hospital policy, and are issuing reminder notices to other departments about the policy. The department has also (1) adopted a policy of not accepting or immediately deleting Social Security numbers received from event organizers; (2) made outreach to the groups and organizations with which it maintains ongoing relationships to request that no social security numbers be sent; (4) established an alternative method of sharing provider billing information internally with staff and ensuring that all copies of the provider listing that included SSNs are destroyed. Finally, we will be providing reinforcement training for the department to reinforce data security policies and ensure that staff understand the risks and requirements around data security, including the importance of adhering to the institution's laptop encryption policy.

Please contact me if you have any questions or concerns, and to discuss logistics of generating the individual notification letters.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Draft Letter to Mass. Resident (Name and SSN specific) w/ offer of Credit Report monitoring services

Date

Name

Address

City/Town/State and Zip

Dear

I am writing to notify you about a possible unauthorized access to or use of your personal information that occurred on or about November 11, 2008, and was identified in late December 2008. We have no indication or evidence that any fraud has been committed or that your personal information has either been retrieved or misused. However, out of an abundance of caution, we wanted to notify you so that you may properly evaluate what actions you may want to consider taking to minimize any potential risks and to protect yourself, as well as what action we plan to take on your behalf. We recommend that you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution.

Under Massachusetts law, you have the right to obtain any police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit report. A security freeze prohibits a credit reporting agency from releasing any information about a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788

Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Found Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or compliant to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit monitoring agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and social security number) **and** the PIN number or password provided to you when you placed the security

freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

In addition, you may place a "fraud alert" on your credit file by contacting the fraud department of any one of the three major credit bureaus. The fraud alert requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three credit bureaus are required by law to automatically send a credit report free of charge to you. This "one-call" fraud alert will remain in your credit file for at least 90 days. When you receive your credit reports, review them carefully for any unexplained activity.

We recommend that you review your credit card and other financial account information regularly for any suspicious or unauthorized activity. *[To help you detect possible misuse of your personal information, we are providing you with a complimentary 2-year membership in Experian's Triple Alert credit monitoring service at no cost to you. This will allow for your credit reports to be monitored at the three national credit reporting companies (Experian, Equifax and TransUnion) and for you to be notified of key changes. You have ninety (90) days to activate this membership, which will then continue for 24 full months. Enrollment in this program will not hurt your credit score. We encourage you to activate your credit monitoring membership as soon as possible.*

The website to enroll in Triple Alert and your individual activation code are both listed below. To sign up, please visit the website and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The website will guide you through the process of enrolling in Triple Alert. If you need technical assistance, please call [insert Experian number].

Triple Alert Website: [insert URL]

Your Activation Code: [insert activation code]

If you wish to enroll over the phone for delivery of your membership via US Mail, please call 8xx-xxx-xxxx.]

Please accept our sincere apologies for this incident. We are committed to protecting confidential and personal information and have taken steps to avoid having this kind of incident happen again. Please contact me if you have any questions about this incident or need further information.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Note: Italicized text will appear only in letters to individuals whose social security number is involved.