From: mail@msgbsvc.com on behalf of ShareThis <donotreply@sharethis.com>
Sent: Tuesday, February 26, 2019 4:08 PM
To: DL-Data Breach Team
Subject: HTML Sample -- Notice of Data Breach

Hello,

At ShareThis, protecting the security of the information in our possession is a responsibility we take very seriously. We write to notify you of a data security incident that may have exposed some of your personal information. This notice explains the incident and steps ShareThis has undertaken to address it. In addition, we provide guidance below on what you can do to protect your personal information.

What Happened?
On February 11, 2019, ShareThis became aware that it suffered a data security incident when it was informed that *The Register* published a story indicating that 16 companies, including ShareThis, were the victims of a data theft. We can tell from our initial investigations that email addresses, hashed passwords and some birth dates were impacted. The incident, unfortunately, only came to light when *The Register* reported that the hacker posted the data for sale on the dark web.

What Information Was Involved?
Although our investigation is ongoing, we believe that the incident occurred in July 2018 and your name, email, date of birth, and hashed password may have been acquired by an unauthorized person or persons. Please note that we have no indication that your password has been used by the hacker or other unauthorized individual. As a result, your personal data may have been compromised.

What We Are Doing.
We value your privacy and deeply regret that this incident occurred. ShareThis will be deactivating any ShareThis accounts associated with this email address. We are reviewing our internal systems and are in the process of working with forensic and data security experts to review this incident and to identify any additional measures we can take to further bolster our security.

What You Can Do.
We want to make sure that you have resources to protect your personal information. As noted above, we deactivated the ShareThis account associated with this email address, so no one will be able to log into it. However, we recommend that you change your password for any other accounts for which you use the same or similar email address or password and take other appropriate steps to protect your online accounts. We also encourage you to be cautious of spam or other phishing emails, including those that solicit personal data. You can also review the **Steps You Can Take to Protect Your Personal Information** below.

Other Important Information.
Maintaining the integrity of confidential information is extremely important to us. We sincerely apologize for any inconvenience this incident may have caused you. We are continuing to investigate this matter and will take appropriate action to prevent future similar incidents.

For More Information.
If you have any questions on this matter, you can email us at inquiries@sharethis.com. You can also visit our website at https://www.sharethis.com/data-privacy-incident.

Sincerely,

Dana Hayes, Jr.
Chief Executive Officer

Steps You Can Take to Protect Your Information

Monitor Your Accounts.
Although we have no reason to believe any financial information of our customers was impacted by this incident, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity to help protect against possible identity theft or other financial loss.

Guard against the possibility of fraud and identity theft.
We suggest you remain as vigilant as ever in monitoring any relevant online accounts or profiles that you may have, particularly for those associated with the same email address. Please consider the complexity of the passwords you use and ensure that you reset and change your passwords for any accounts which have the same or similar passwords. If you do notice any suspicious activity on any online accounts, contact your account provider immediately.

Stay alert to the risk of malicious emails. We recommend that you continue to be vigilant against malicious emails such as phishing emails, including by considering whether you are expecting a particular email, confirming the full email address and domain of the sender, as well as looking out for spelling mistakes, suspicious links and other signs that the message is suspicious. If you think you may have divulged personal information (including any log-in credentials) as a result of a phishing email, please immediately change those credentials.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. If you would like to order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. Although ShareThis does not ask for, or collect or maintain in any way, Social Security numbers for our customers, we advise you that you have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian **P.O. Box 9554** **Allen, TX 75013** **1-888-397-3742** **www.experian.com/fraud/center.html**	**TransUnion** **P.O. Box 2000** **Chester, PA 19106** **1-800-909-8872** **www.transunion.com/fraud-victim-resource/place-fraud-alert**	**Equifax** **P.O. Box 105788** **Atlanta, GA 30348-5788** **1-800-685-111** **www.equifax.com/personal/credit-report-services**

In order to request a security freeze, you will need to supply 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 complaint to a law enforcement agency concerning identity theft.

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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by law enforcement. ***For Rhode Island Residents***: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. The number of Rhode Island residents impacted by this event is unable to be determined.

If you would prefer not to receive further messages from this sender, please Click Here and confirm your request. 

From: mail@msgbsvc.com on behalf of ShareThis <donotreply@sharethis.com>
Sent: Tuesday, February 26, 2019 3:35 PM
To: DL-Data Breach Team
Subject: HTML Sample -- Notice of Data Breach

Hello,

At ShareThis, protecting the security of the information in our possession is a responsibility we take very seriously. We write to notify you of a data security incident that may have exposed some of your personal information. This notice explains the incident and steps ShareThis has undertaken to address it. In addition, we provide guidance below on what you can do to protect your personal information.

What Happened?
On February 11, 2019, ShareThis became aware that it suffered a data security incident when it was informed that *The Register* published a story indicating that 16 companies, including ShareThis, were the victims of a data theft. We can tell from our initial investigations that email addresses, hashed passwords and some birth dates were impacted. The incident, unfortunately, only came to light when *The Register* reported that the hacker posted the data for sale on the dark web.

What Information Was Involved?
Although our investigation is ongoing, we believe that the incident occurred in July 2018 and your name, email and hashed password may have been acquired by an unauthorized person or persons. Please note that we have no indication that your password has been used by the hacker or other unauthorized individual. As a result, your personal data may have been compromised.

What We Are Doing.
We value your privacy and deeply regret that this incident occurred. ShareThis will be deactivating any ShareThis accounts associated with this email address. We are reviewing our internal systems and are in the process of working with forensic and data security experts to review this incident and to identify any additional measures we can take to further bolster our security.

What You Can Do.
We want to make sure that you have resources to protect your personal information. As noted above, we deactivated the ShareThis account associated with this email address, so no one will be able to log into it. However, we recommend that you change your password for any other accounts for which you use the same or similar email address or password and take other appropriate steps to protect your online accounts. We also encourage you to be cautious of spam or other phishing emails, including those that solicit personal data. You can also review the **Steps You Can Take to Protect Your Personal Information** below.

Other Important Information.
Maintaining the integrity of confidential information is extremely important to us. We sincerely apologize for any inconvenience this incident may have caused you. We are continuing to investigate this matter and will take appropriate action to prevent future similar incidents.

For More Information.
If you have any questions on this matter, you can email us at inquiries@sharethis.com. You can also visit our website at https://www.sharethis.com/data-privacy-incident.

Sincerely,

Dana Hayes, Jr.
Chief Executive Officer

Steps You Can Take to Protect Your Information

Monitor Your Accounts.
Although we have no reason to believe any financial information of our customers was impacted by this incident, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity to help protect against possible identity theft or other financial loss.

Guard against the possibility of fraud and identity theft.
We suggest you remain as vigilant as ever in monitoring any relevant online accounts or profiles that you may have, particularly for those associated with the same email address. Please consider the complexity of the passwords you use and ensure that you reset and change your passwords for any accounts which have the same or similar passwords. If you do notice any suspicious activity on any online accounts, contact your account provider immediately.

Stay alert to the risk of malicious emails. We recommend that you continue to be vigilant against malicious emails such as phishing emails, including by considering whether you are expecting a particular email, confirming the full email address and domain of the sender, as well as looking out for spelling mistakes, suspicious links and other signs that the message is suspicious. If you think you may have divulged personal information (including any log-in credentials) as a result of a phishing email, please immediately change those credentials.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. If you would like to order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. Although ShareThis does not ask for, or collect or maintain in any way, Social Security numbers for our customers, we advise you that you have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian **P.O. Box 9554** **Allen, TX 75013** **1-888-397-3742** **www.experian.com/fraud/center.html**	**TransUnion** **P.O. Box 2000** **Chester, PA 19106** **1-800-909-8872** **www.transunion.com/fraud-victim-resource/place-fraud-alert**	**Equifax** **P.O. Box 105788** **Atlanta, GA 30348-5788** **1-800-685-111** **www.equifax.com/personal/credit-report-services**

In order to request a security freeze, you will need to supply 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 complaint to a law enforcement agency concerning identity theft.

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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by law enforcement. ***For Rhode Island Residents***: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. The number of Rhode Island residents impacted by this event is unable to be determined.

If you would prefer not to receive further messages from this sender, please Click Here and confirm your request.