

July 16, 2021

Tawana B. Johnson, Esq.
470.419.6653 (direct)
Tawana.Johnson@WilsonElser.com

Via electronic-mail: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Attorney General Gordon McDonald

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Our Client : Broken Sound Club, Inc.
Matter : Data Security Incident on March 26, 2021
Wilson Elser File # : 16516.01411

Dear Attorney General McDonald:

We represent Broken Sound Club, Inc. (“BSC”) headquartered in Boca Raton, Florida with respect to a data security incident described in more detail below. BSC takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that BSC is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On March 26, 2021, BSC was the target of a ransomware attack that may have resulted in the exposure of personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals’ names, mailing addresses, W-9 and/or social security numbers could have been exposed as a result of this attack.

As of this writing, BSC has not received any reports of related identity theft since the date of the incident (March 26, 2021 to present).

3348 Peachtree Road, N.E., Suite 1400, Atlanta, Georgia 30326

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Kentucky • Las Vegas
London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Diego • San Francisco • Stamford
Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com

2. Number of New Hampshire Residents Affected

A total of two (2) residents of New Hampshire were potentially affected by this security incident. A notification letter to these individuals will be mailed on July 16, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, BSC contacted a reputable 3rd party forensic team to assist with its investigation. Since then, BSC has been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of BSC's systems.

Although BSC is not aware of any evidence of misuse of personal information, BSC extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. With this protection, IDX will help the affected individuals resolve issues if their identity is compromised.

4. Contact Information

BSC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Tawana.Johnson@WilsonElser.com or 470.419.6653.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Tawana B. Johnson, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)
Michael Kar, Esq.

Enclosure: *Sample Notification Letter*

3348 Peachtree Road, N.E., Suite 1400, Atlanta, Georgia 30326

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Kentucky • Las Vegas
London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Diego • San Francisco • Stamford
Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing in order to inform you of an incident that may have exposed your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On March 26, 2021, Broken Sound Club, Inc. (“BSC”) detected a data security incident. An unauthorized third party attempted to lock us out of our network environment in exchange for a financial payment to resume business operations. We immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the environment.

We also initiated a comprehensive investigation into what sensitive data could have been compromised. Although we have no evidence that any personal information has been misused, our forensic investigation determined that your full name, mailing address, and/or social security number could have been compromised during the incident. We maintained this information for our members and their families for purposes of payment processing and the provision of member services at the club.

As of this writing, BSC has not received any reports of related identity theft since the date of the incident (March 26, 2021 to present).

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate our incident response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have been working with law enforcement to respond to this incident. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We have also secured free identity monitoring services for all affected individuals, as set forth in full below.

What You Can Do:

We value the safety of your personal information and are therefore offering identity monitoring services through Kroll, a global leader in risk mitigation and response. Kroll’s services include: 12 months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **September 27, 2021** to activate your identity monitoring services.*

Membership Number: <<subscriber_number>>

Additional information describing your services is included with this letter.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding monitoring your personal information.

For More Information:

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further help protect your personal information.

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Kroll services at [1-800-870-8700](tel:1-800-870-8700), Monday through Friday, 8:00am – 5:30pm CT, excluding major U.S. national holidays.

Broken Sound Club, Inc. values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "John Crean".

John Crean
General Manager and COO
Broken Sound Club, Inc.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<http://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right

to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you’ll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing in order to inform you of an incident that may have exposed your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On March 26, 2021, Broken Sound Club, Inc. (“BSC”) detected a data security incident. An unauthorized third party attempted to lock us out of our network environment in exchange for a financial payment to resume business operations. We immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the environment.

We also initiated a comprehensive investigation into what sensitive data could have been compromised. Although we have no evidence that any personal information has been misused, our forensic investigation determined that your full name, mailing address, W-9 and/or Social Security number could have been compromised during the incident. We maintained this information for our vendors on our system for standard business purposes.

As of this writing, BSC has not received any reports of related identity theft since the date of the incident (March 26, 2021 to present).

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate our incident response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have been working with law enforcement to respond to this incident. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We have also secured free identity monitoring services for all affected individuals, as set forth in full below.

What You Can Do:

We value the safety of your personal information and are therefore offering identity monitoring services through Kroll, a global leader in risk mitigation and response. Kroll’s services include: 12 months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **September 27, 2021** to activate your identity monitoring services.*

Membership Number: <<subscriber_number>>

Additional information describing your services is included with this letter.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full

advantage of this service offering. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding monitoring your personal information.

For More Information:

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further help protect your personal information.

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Kroll services at [1-800-870-8700](tel:1-800-870-8700), Monday through Friday, 8:00am – 5:30pm CT, excluding major U.S. national holidays.

Broken Sound Club, Inc. values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "John Crean".

John Crean
General Manager and COO
Broken Sound Club, Inc.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<http://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right

to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you’ll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.