



Christopher J. Dilenno
D: 215.358.5161
C: 610.283.5286
cdiianno@nldhlaw.com

518 Township Line Road
Suite 300
Blue Bell, PA 19422
P: 215.358.5100
F: 215.358.5101

May 23, 2013

Attorney General Michael A. Delaney
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Beachbody, LLC — Notice of Data Security Event

Dear Sir or Madam:

We represent Beachbody, LLC (“Beachbody”), 3301 Exposition Boulevard, 3rd Floor, Santa Monica, CA 90404, and are writing to notify you of a data event that compromised the security of personal information of one hundred sixty one (161) New Hampshire residents. Beachbody’s investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Beachbody does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

In late March and early April of 2013, Beachbody received reports from some of its customers that they were experiencing fraudulent purchases on credit cards used for online purchases at a Beachbody website. Around April 6, 2013, Beachbody retained forensic experts, Kroll, Inc. (“Kroll”), to investigate its systems and determine whether its databases were secure. On April 17, 2013, Beachbody learned that an unknown unauthorized individual(s) had hacked into one of Beachbody’s websites and had access to a database containing the first and last name, email address, mailing address, telephone number, credit card number and CVV number of certain website customers.

In addition to retaining our firm and Kroll, Beachbody reported this incident to the United States Secret Service. Beachbody is assisting with the Secret Service’s ongoing investigation into this incident. Beachbody notified its payment processor and retained a second independent forensics expert, Trustwave, in order to confirm compliance of all systems with payment card industry standards. These investigations are ongoing.

Notice to New Hampshire Residents

Although the investigations are ongoing, it appears that the personal information of one hundred sixty one (161) New Hampshire residents was potentially accessed as a result of this data event. Beachbody sent an email to these New Hampshire residents, providing information regarding the incident and notice that the resident would also receive a written letter from Beachbody regarding the event. *See, Exhibit A.* These New Hampshire residents were sent this written notice on or about May 16, 2013, in substantially the same form as the letter attached here at *Exhibit B.*

Other Steps Taken and To Be Taken

In addition to providing the email and written notice of this incident to all affected individuals as described above, Beachbody posted notice of this incident and Frequently Asked Questions on its website. *See, Exhibit C.* Each affected customer is being offered access to one (1) free year of credit monitoring services and identity restoration services. Beachbody is also providing each individual with information on how to protect against identity theft and fraud. Beachbody is providing written notice of this incident to other state and international regulators, and to the national consumer reporting agencies. In addition to retaining its two forensic vendors to confirm the scope of the unauthorized access and the security of the Beachbody system, Beachbody terminated access to the vulnerable website and created a new secure website that is designed to prevent a recurrence of such an incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-358-5161.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. DiLenno', with a stylized flourish at the end.

Christopher J. DiLenno, Esquire

cc: Beachbody, LLC

EXHIBIT A



3301 Exposition Blvd., Third Floor
Santa Monica, California 90404

May 10, 2013

Dear Powder Blue customer:

Unfortunately, it has come to our attention that someone hacked into the Powder Blue website and obtained access to some of our customers' credit card numbers (there were no social security numbers in the affected database). I sincerely apologize for any aggravation or concern that this may cause. Please know that we treat the security of our customers' personal information as a top priority and we are doing everything we can, including working with local law enforcement, the Secret Service, specialized outside legal counsel and forensic security experts to investigate exactly how this illegal attack occurred, to conduct a criminal investigation, and to ensure that all Powder Blue systems will be just as secure as the other Beachbody systems going forward. [Click here](#) for specific FAQs (Frequently Asked Questions) which further detail the information related to these ongoing investigations, how to best protect yourself against any unauthorized charges, and what Beachbody is doing to protect you and all of our other Powder Blue customers.

As an immediate step to protect against potentially unauthorized charges, we suggest that you call the bank or credit card company (there is usually a phone number on the back of any credit or debit card) which you used to purchase Powder Blue products over the past year. Please explain this notice to them and ask that you want to be issued a new card number because your credit card information may have been compromised. We also encourage you to carefully review your statements tied to these cards and report any unauthorized charges to your bank or credit card company.

Working with our experts, we have addressed and fixed the vulnerabilities which caused this problem. And while in this age of cyberattacks and changing technology no one can guarantee that future attacks by online criminals will not occur, rest assured that we are working diligently to help ensure that this does not happen again. Please also know that we have thoroughly investigated all of our Beachbody systems and have concluded that all of the other Beachbody systems, which are maintained separately from the Powder Blue system, are secure and we have found no fraudulent activity or security breaches with any Team Beachbody Coach, Shakeology, or other Beachbody orders.

As required by laws in all states where our customers were affected, we will be contacting all of our affected Powder Blue customers by U.S. Mail shortly. That letter will detail how to enroll in credit monitoring services for our affected Powder Blue customers, as well as credit restoration services for any Powder Blue customer who has been the victim of actual fraud as a result of using the Powder Blue website. For a copy of this letter which also includes the FAQ, please [click here](#).

Most importantly, I am truly sorry for this inconvenience. Providing the best customer experience is crucial for Beachbody and me, especially as we work together to help you grow your certification business. I genuinely appreciate your support and understanding while we address and remedy the problems these criminals may have created for us all and I will work even harder to keep your business and reward your loyalty.

Sincerely,

Carl Daikeler
Chief Executive Officer

EXHIBIT B



BEACHBODY

Decide. Commit. Succeed.®

<<Firstname>> <<Middlename>> <<Lastname>>

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

<<Address1>>

<<Address2>>

<<City>>, <<Stateprovince>> <<Postalcode>>

<<Intelligent Mail Barcode>>

Dear <<Firstname>> <<Middlename>> <<Lastname>>,

We sent an email to you on May X, 2013, to advise you of an incident that may affect the security of your personal information. We are unaware of any attempted or actual misuse of your personal information, but are providing you additional information relating this incident to ensure that you are aware of the incident and so that you may take steps to monitor your identity, and your credit accounts, should you feel it is necessary to do so.

On April 17, 2013, Beachbody became aware that an unknown unauthorized individual(s) hacked into the Powder Blue website. Upon learning that the Powder Blue website had been compromised, Beachbody immediately commenced an internal investigation. Beachbody retained privacy and data legal counsel to assist in its investigations and response to this incident. Beachbody retained third-party forensic experts, Kroll Advisory Solutions ("Kroll"), to identify vulnerabilities on the Powder Blue website. Kroll also assisted Beachbody in identifying the specific data exposed and the individuals affected by this incident. At this time, Kroll determined that your credit card number, email address, mailing address, telephone number, first name, last name, and CVV number were potentially accessed. No social security numbers were in this database.

Beachbody takes this matter, and the security of your personal information, seriously. Upon discovering a potential issue with the Powder Blue website, in addition to launching its own internal investigation and retaining Kroll to perform an independent forensic investigation, Beachbody retained a second computer forensic company to ensure that all Powder Blue systems are in compliance with payment card industry standards and to ensure all affected individuals have been identified. Beachbody is also working with the United States Secret Service with its investigation into this incident. Although these investigations are ongoing, at this time we have no evidence to suggest that any of our computer systems outside of the Powder Blue website have been compromised. This notice was not delayed because of law enforcement.

We retained Kroll to provide—at no cost to you—one year of its credit monitoring and identity restoration services under its **ID TheftSmart™** program. Kroll is a global leader in risk mitigation and response, and has years of experience when it comes to helping people who have sustained an unintentional exposure of confidential data.

Kroll's **ID TheftSmart** program includes Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration:

Continuous Credit Monitoring. Beachbody is providing you with no-cost access to Kroll's credit monitoring service for 12 months from the date of this letter. Once activated, you will receive alerts whenever there are certain changes in your credit files, maintained by Experian, Equifax, and TransUnion, that could indicate suspicious activity.

Enhanced Identity Theft Consultation and Restoration. Licensed investigators, who understand the problems surrounding identity theft, are available to answer your questions, at no cost, and to offer their expertise regarding any concerns you may have. Should your name and credit be affected by this incident, your investigator will help restore your identity to pre-theft status.

To receive credit monitoring, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

In order to receive credit services, you must follow one of two steps:

1. **VISIT www.idintegrity.com.** Provide your unique membership number: <<MembershipNumber>>, last name, and zip code; for non-military U.S. citizens living abroad use zip code: 00000.
2. If you would prefer to receive your alerts through the mail instead of online, fill out the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form* and return it in the enclosed postage-paid envelope. This option is not available to United States citizens living abroad.

We have established a confidential assistance line for you to utilize if you have any questions or concerns regarding the incident or the contents of this letter, or if you believe you may be a victim of identity theft. This confidential assistance line is staffed with professionals trained in identity and credit safeguard and restoration. These professionals are also familiar with this incident, and can provide you with additional information concerning this incident. You may reach the confidential assistance line by dialing, toll-free, (855) 269-6545 Monday through Friday, 8:00 a.m. to 5:00 p.m. C.D.T., excluding major holidays. Please have your unique membership number (above) available when calling.

The enclosed "U.S. State Notification Requirements" sheet provides additional information on how to protect against identity theft and fraud. This sheet also contains the contact information for state and federal agencies, as well as the three national credit reporting agencies.

We apologize for any inconvenience or concern that this may have caused you. The safety and security of your personal information remains a top priority of Beachbody. Please do not hesitate to take advantage of Kroll's **IDTheftSmart** program and to contact the privacy line should you have any questions.

Very truly yours,

Carl Daikeler
Chief Executive Officer, Beachbody

EXHIBIT C



3301 Exposition Blvd., Third Floor
Santa Monica, California 90404

May 10, 2013

Dear Powder Blue customer:

Unfortunately, it has come to our attention that someone hacked into the Powder Blue website and obtained access to some of our customers' credit card numbers (there were no social security numbers in the affected database). I sincerely apologize for any aggravation or concern that this may cause. Please know that we treat the security of our customers' personal information as a top priority and we are doing everything we can, including working with local law enforcement, the Secret Service, specialized outside legal counsel and forensic security experts to investigate exactly how this illegal attack occurred, to conduct a criminal investigation, and to ensure that all Powder Blue systems will be just as secure as the other Beachbody systems going forward. Attached to this email are FAQs (Frequently Asked Questions) which further detail the information related to these ongoing investigations, how to best protect yourself against any unauthorized charges, and what Beachbody is doing to protect you and all of our other Powder Blue customers.

As an immediate step to protect against potentially unauthorized charges, we suggest that you call the bank or credit card company (there is usually a phone number on the back of any credit or debit card) which you used to purchase Powder Blue products over the past year. Please explain this notice to them and ask that you want to be issued a new card number because your credit card information may have been compromised. We also encourage you to carefully review your statements tied to these cards and report any unauthorized charges to your bank or credit card company.

Working with our experts, we have addressed and fixed the vulnerabilities which caused this problem. And while in this age of cyberattacks and changing technology no one can guarantee that future attacks by online criminals will not occur, rest assured that we are working diligently to help ensure that this does not happen again. Please also know that we have thoroughly investigated all of our Beachbody systems and have concluded that all of the other Beachbody systems, which are maintained separately from the Powder Blue system, are secure and we have found no fraudulent activity or security breaches with any Team Beachbody Coach, Shakeology, or other Beachbody orders.

As required by laws in all states where our customers were affected, we will be contacting all of our affected Powder Blue customers by U.S. Mail shortly. That letter will detail how to enroll in credit monitoring services for our affected Powder Blue customers, as well as credit restoration services for any Powder Blue customer who has been the victim of actual fraud as a result of using the Powder Blue website.

Most importantly, I am truly sorry for this inconvenience. Providing the best customer experience is crucial for Beachbody and me, especially as we work together to help you grow your certification business. I genuinely appreciate your support and understanding while we address and remedy the problems these criminals may have created for us all and I will work even harder to keep your business and reward your loyalty.

Sincerely,

Carl Daikeler
Chief Executive Officer



May 10, 2013

Powder Blue Cyber-Attack Frequently Asked Questions

1. What happened?

While we are still investigating, Beachbody recently determined that the Powder Blue database was hacked by unknown individuals. It appears that the hackers inserted a backdoor “web shell” on Powder Blue’s web site, which allowed the hackers to potentially access and obtain customer personal information.

2. What personal information was exposed?

The following Powder Blue customer data was exposed as a result of this attack: Email address, mailing address, telephone number, first name, last name, credit card number, and CVV number. No social security numbers were in this database.

3. Were any other Beachbody databases attacked? (If I am a Coach and drink Shakeology®, should I be concerned?)

No. We have done thorough security testing and have concluded that all of the other Beachbody systems, which are maintained separately from the Powder Blue system, are secure. We have found no fraudulent activity or security breaches with any Team Beachbody Coach, Shakeology, or other Beachbody orders.

4. Did Beachbody investigate the attack?

Beachbody began an internal investigation into the attack immediately after it was notified of security concerns by our Powder Blue customers. As soon as we validated a security concern, we contacted a number of law enforcement agencies, including the United States Secret Service, and engaged nationally recognized independent computer forensic experts and independent privacy and data security legal counsel to assist us in aggressively investigating and responding to this incident.

5. Why did it take so long to notify me?

Upon learning of this suspected cyber-attack, Beachbody took steps to immediately investigate and respond. The investigation required a thorough and complete analysis to accurately identify the precise type and scope of the cyber-attack, the data potentially exposed, and the customers who were potentially affected by the suspected cyber-attack. To assist with its investigation, Beachbody retained two different independent, third-party computer forensic expert companies to conduct its investigation, as well as to comply with banking requirements to ensure that the system is compliant with payment card standards and all affected individuals have been identified. Beachbody additionally retained specialized legal counsel to assist in its investigation and response to this incident and to ensure that Beachbody's response complies with all statutory and regulatory legal obligations relating to data events.

During our investigation Beachbody contacted a number of law enforcement agencies, including the United States Secret Service. Beachbody continues to cooperate with the Secret Service in order to move forward with any potential criminal proceedings. Once our investigation confirmed the exposure of customer information, in line with regulatory requirements, Beachbody immediately began preparing notices to all affected customers. We are in the process of arranging for affected customers to receive credit monitoring and identity restoration services for free for one year and will be providing enrollment instructions for these services as well as additional details in a statutory notice that will be sent to you via US mail soon (if we do not have your current postal address, please see the customer service contact information at the end of this FAQ).

6. Was Powder Blue's network security insufficient at the time of attack?

Unfortunately, many companies face hacking attacks every day. Like so many others – from the world's largest financial sites to Facebook – we were not immune. Fortunately, because of the security measures we had in place, we were able to shut this attack down quickly and investigate thoroughly to understand precisely what happened and who was affected. In today's information driven world and economy, there will always be risks for cybercrime. No companies are immune from it, but all companies have to be prepared for it.

We sincerely apologize for any inconvenience or frustration that this may have caused you. We value your business, and remain committed to maintaining the security of your personal information.

7. What other protective measures does Beachbody have in place and is it safe placing another order?

We have network security measures in place that work to protect us against malicious online attacks and warn us when an attack occurs, including protection behind a firewall. We also have physical and procedural safeguards in place that protect, and limit access, to customer and user information. In addition, following this attack, we are implementing enhanced network security

measures, which are stringent and state of the art, employing the best resources available both internally and externally to protect all customer information.

8. Were Social Security numbers accessed?

No. Beachbody does not ask for or require our customers to provide social security numbers so they were never in the affected database.

9. How can you be sure that you are right about the information that was and was not compromised?

Our IT team measured the impact of this attack through extensive testing and monitoring methods. Further, our independent security auditors are performing their own network tests and investigation and verifying our conclusions.

10. How do I know if I was affected by this incident and will this affect my current orders or continuities with Powder Blue?

We are providing email and/or written notice of this incident to the last known contact information of all customers in the affected Powder Blue database whose information may be at risk as a result of this incident. This will not affect anybody's pending orders, VIP status or continuity workouts and music.

11. What should I do to protect myself?

We encourage all Powder Blue customers to call the banks and credit card companies that issued any credits cards used to purchase Powder Blue products, discuss this matter with them, and request new card numbers and new credit cards. We encourage all Powder Blue customers to change account passwords, refrain from sharing account passwords and other user credentials, and refrain from opening any email or link sent from an unknown sender.

Beachbody also encourages users to remain vigilant in reviewing account statements and reviewing credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You can also obtain your free credit report directly from any one or more of the three national consumer reporting agencies.

The contact information for these agencies is:

Equifax, PO Box 105069, Atlanta, GA 30348, 800-525-6285, www.equifax.com
Experian, PO Box 2104, Allen, TX 75013, 888-397-3742, www.experian.com
TransUnion, PO Box 6790, Fullerton, CA 92834, 800-680-7289, www.transunion.com

At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. However, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the credit agencies.

The Federal Trade Commission has also compiled helpful information on steps you can take to avoid or detect identity theft. You can visit the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/ or call their toll-free hotline at 877-ID-THEFT (438-4338).

12. Even if I haven't seen any fraudulent activity, should I still check my credit report?

Yes. It's always a good idea to check your credit report, regardless of whether you've been a victim of identity theft or fraud, and regardless of whether your personal information has been exposed. Every consumer can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com.

13. Is Beachbody offering its users identity or credit monitoring services?

Yes, though we were not obligated to, for our customers' peace of mind, we are offering users whose information may be at risk as a result of this attack one (1) free year of access to the following service, with instructions on how to enroll to be provided to all affected customers in the mail shortly following this email:

Triple Credit bureau monitoring will be available through the 3 national credit report agencies. If you choose this service, you may either access it immediately online or by completing the Credit Authorization Form. This service will monitor your credit activity and promptly report to you any activity involving a new inquiry, new trade line, new derogatory information, new public record or change of address. This service will not affect your credit score nor will it appear as a hard inquiry on your credit report when the credit report is accessed by a third party.

14. There are fraudulent charges on my credit/debit card. What do I do?

If you have fraudulent charges on your credit or debit card, you should immediately contact the financial institution that issued the card and let them know about the unauthorized charges. They will provide you with the instructions to have the unauthorized charges disputed and how to have

a new account issued to avoid any further unauthorized activity. Also, you may wish to report any instance of suspected identity theft to law enforcement.

15. Does this mean I am a victim of identity theft?

Not necessarily. The fact that an unauthorized individual had access to your personal information does not mean that you are a victim of identity theft, or that the information accessed will be used to commit fraud. Identity theft occurs when a person who is not you uses your personal information fraudulently, beyond only fraudulently charging on your credit or debit card.

16. I have been the victim of identity theft. What services can you offer me?

We will be offering credit restoration services to those Powder Blue customers who are the victims of fraud as a result of using the Powder Blue website to assist in restoring any credit or identity attacks for those affected to the pre-theft status. We will provide our affected customers instructions on how to obtain credit restoration services in the postal letter which will be sent shortly.

17. I am a Powder Blue customer and am trying to get more information. How do I do so?

Please contact our security response call center at 1-855-269-6545, which will be open Monday through Friday from 8 AM to 5 PM Central.

18. I work with the media and am trying to get more information. How do I do so?

Please contact Beachbody's Chief Legal Officer, Jonathan Gelfand, at jonathan@beachbody.com.

19. I work with law enforcement and am trying to get more information. How do I do so?

Please contact Beachbody's VP of Legal Affairs, Steve Moran smoran@beachbody.com or (310) 883-9202.

2013 MAY 21 11:12 38

DEPT OF JUSTICE
STATE OF NH