

# BakerHostetler

## Baker&Hostetler LLP

312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202-4074

T 513.929.3400  
F 513.929.0303  
www.bakerlaw.com

Patrick H. Haggerty  
direct dial: 513.929.3412  
phaggerty@bakerlaw.com

March 8, 2017

### VIA EMAIL (CONSUMER@IOWA.GOV) AND OVERNIGHT MAIL

Consumer Protection Division  
Security Breach Notifications  
Office of the Attorney General of Iowa  
1305 E. Walnut Street  
Des Moines, Iowa 50319

*Re: Incident Notification*

Dear Sir or Madam:

Our client, prAna, understands the importance of protecting the personal information provided by its customers. On February 6, 2017, prAna detected that an unauthorized third party may have obtained access to the servers that operate its e-commerce website, [www.pрана.com](http://www.pрана.com). prAna quickly began an investigation and hired a leading cybersecurity firm to assist in the investigation and remediate the website. prAna has notified the FBI and will cooperate with any ensuing investigation.

Findings from the investigation show that an unauthorized third party installed code that was designed to capture information as it was being entered on the site during the checkout process for orders placed from December 14, 2016 to February 6, 2017. prAna believes the unauthorized third party may have also decrypted an internal database containing information from orders completed prior to February 6, 2017. The information that may have been affected includes customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV), and username and account password for the website.

As part of its efforts to address this issue, prAna is requiring users to change their passwords for potentially affected customers that have a prAna.com account. If such customers use the same username and password for any other account, prAna is recommending that the customers change their password there as well. In addition, prAna has provided a toll-free number that potentially affected customers can call with questions regarding the incident. prAna

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

March 8, 2017

Page 2

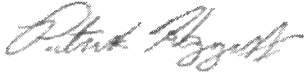
is also recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

Today, prAna is beginning to send written notification via U.S. Mail to 2,335 Iowa residents in accordance with Iowa Code § 715C.1-2 in substantially the same form as the letter attached hereto.<sup>1</sup> Notice is being provided as expeditiously as practicable and without unreasonable delay.

To help prevent this type of incident from happening again, prAna has remediated the e-commerce website and continues to work to strengthen the security of its e-commerce website.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Patrick H. Haggerty  
Partner

Enclosure

---

<sup>1</sup> This report is not, and does not constitute, a waiver of personal jurisdiction.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

**RE: Your payment card ending in <<credit card last 4 digits>>**

Dear <<Name>>,

At prAna, we value our relationship with our customers and understand the importance of protecting personal information. We are writing to inform you about an incident that may involve some of that information, including your payment card information.

On February 6, 2017, we detected that an unauthorized third party may have obtained access to the servers that operate our e-commerce website, [www.pрана.com](http://www.pрана.com). We immediately hired a leading cybersecurity firm to assist us in our investigation and remediate the website. We have notified the FBI and will cooperate with any ensuing investigation.

Findings from the investigation show that an unauthorized third party captured information as it was being entered on the site during the checkout process for orders placed from December 14, 2016 to February 6, 2017. Based on our investigation, we believe the unauthorized third party also may have decrypted an internal database containing information from completed orders prior to February 6, 2017. The information that may have been affected includes your name, address, phone number, email address, payment card number ending in <<last 4 digits>>, expiration date and security code (CVV), and username and account password for our website.

We encourage that you remain vigilant to the possibility of fraud by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. You should also review the additional information on the following page on ways to protect yourself.

If you have a prAna.com account, for your security you will need to reset your password before you are able to use your account. Also, if you use the same username and password for any other account, we recommend that you change your password there as well.

We apologize for any inconvenience or concern this may have caused. To help prevent this type of incident from happening again, we are continuing to take steps to strengthen the security of our e-commerce website.

If you have questions, please call 1-844-685-5625, Monday through Friday, from 9 a.m. to 9 p.m. EST (closed on U.S. observed holidays).

Sincerely,

Scott Kerslake  
CEO, prAna

**MORE INFORMATION ON WAYS TO PROTECT YOURSELF**  
*NOTICE AS REQUIRED BY STATE LAW*

It is recommended that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

## AG CONSUMER [AG]

---

**From:** Kenaley, Patricia <pkenaley@bakerlaw.com>  
**Sent:** Wednesday, March 08, 2017 1:33 PM  
**To:** AG CONSUMER [AG]  
**Cc:** Haggerty, Patrick H.  
**Subject:** prAna - Incident Notification  
**Attachments:** IA AG notice ltr. - prana.pdf

Please see the attached incident notification.

Sent on behalf of:

**Pat Haggerty**  
Partner

---

**BakerHostetler**  
312 Walnut Street | Suite 3200  
Cincinnati, OH 45202-4074  
T 513.929.3412

phaggerty@bakerlaw.com  
bakerlaw.com



---

This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

Any tax advice in this email is for information purposes only. The content of this email is limited to the matters specifically addressed herein and may not contain a full description of all relevant facts or a complete analysis of all relevant issues or authorities.

Internet communications are not assured to be secure or clear of inaccuracies as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Therefore, we do not accept responsibility for any errors or omissions that are present in this email, or any attachment, that have arisen as a result of e-mail transmission.

# BakerHostetler

## Baker & Hostetler LLP

312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202-4074

T 513.929.3400  
F 513.929.0303  
www.bakerlaw.com

Patrick H. Haggerty  
direct dial: 513.929.3412  
phaggerty@bakerlaw.com

March 8, 2017

### VIA EMAIL (CONSUMER@IOWA.GOV) AND OVERNIGHT MAIL

Consumer Protection Division  
Security Breach Notifications  
Office of the Attorney General of Iowa  
1305 E. Walnut Street  
Des Moines, Iowa 50319

Re: *Incident Notification*

Dear Sir or Madam:

Our client, prAna, understands the importance of protecting the personal information provided by its customers. On February 6, 2017, prAna detected that an unauthorized third party may have obtained access to the servers that operate its e-commerce website, [www.pрана.com](http://www.pрана.com). prAna quickly began an investigation and hired a leading cybersecurity firm to assist in the investigation and remediate the website. prAna has notified the FBI and will cooperate with any ensuing investigation.

Findings from the investigation show that an unauthorized third party installed code that was designed to capture information as it was being entered on the site during the checkout process for orders placed from December 14, 2016 to February 6, 2017. prAna believes the unauthorized third party may have also decrypted an internal database containing information from orders completed prior to February 6, 2017. The information that may have been affected includes customer's name, address, phone number, email address, payment card number, expiration date and security code (CVV), and username and account password for the website.

As part of its efforts to address this issue, prAna is requiring users to change their passwords for potentially affected customers that have a prAna.com account. If such customers use the same username and password for any other account, prAna is recommending that the customers change their password there as well. In addition, prAna has provided a toll-free number that potentially affected customers can call with questions regarding the incident. prAna

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

RECEIVED  
7 MAR -9 AM 10:19  
CONSUMER PROTECTION DIV.

March 8, 2017

Page 2

is also recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

Today, prAna is beginning to send written notification via U.S. Mail to 2,335 Iowa residents in accordance with Iowa Code § 715C.1-2 in substantially the same form as the letter attached hereto.<sup>1</sup> Notice is being provided as expeditiously as practicable and without unreasonable delay.

To help prevent this type of incident from happening again, prAna has remediated the e-commerce website and continues to work to strengthen the security of its e-commerce website.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Patrick H. Haggerty  
Partner

Enclosure

---

<sup>1</sup> This report is not, and does not constitute, a waiver of personal jurisdiction.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

**RE: Your payment card ending in <<credit card last 4 digits>>**

Dear <<Name>>,

At prAna, we value our relationship with our customers and understand the importance of protecting personal information. We are writing to inform you about an incident that may involve some of that information, including your payment card information.

On February 6, 2017, we detected that an unauthorized third party may have obtained access to the servers that operate our e-commerce website, [www.pрана.com](http://www.pрана.com). We immediately hired a leading cybersecurity firm to assist us in our investigation and remediate the website. We have notified the FBI and will cooperate with any ensuing investigation.

Findings from the investigation show that an unauthorized third party captured information as it was being entered on the site during the checkout process for orders placed from December 14, 2016 to February 6, 2017. Based on our investigation, we believe the unauthorized third party also may have decrypted an internal database containing information from completed orders prior to February 6, 2017. The information that may have been affected includes your name, address, phone number, email address, payment card number ending in <<last 4 digits>>, expiration date and security code (CVV), and username and account password for our website.

We encourage that you remain vigilant to the possibility of fraud by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. You should also review the additional information on the following page on ways to protect yourself.

If you have a prAna.com account, for your security you will need to reset your password before you are able to use your account. Also, if you use the same username and password for any other account, we recommend that you change your password there as well.

We apologize for any inconvenience or concern this may have caused. To help prevent this type of incident from happening again, we are continuing to take steps to strengthen the security of our e-commerce website.

If you have questions, please call 1-844-685-5625, Monday through Friday, from 9 a.m. to 9 p.m. EST (closed on U.S. observed holidays).

Sincerely,

Scott Kerslake  
CEO, prAna



**MORE INFORMATION ON WAYS TO PROTECT YOURSELF**  
*NOTICE AS REQUIRED BY STATE LAW*

It is recommended that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

Extremely Urgent

This envelope is for use with the following services: UPS Next Day Air®  
UPS Worldwide Express®  
UPS 2nd Day Air®

Documents  
in the top.

Page 1 of 1

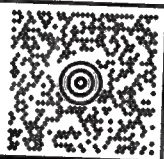
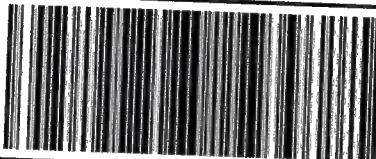
Visit [ups.com](http://ups.com) or call 1-800-  
to schedule a pickup or for

**Domestic Shipments**  
• To qualify for the Letter rate,  
correspondence, urgent  
weigh 8 oz. or less, UP  
those listed or weighing.

**International Shipments**  
• The UPS Express Envelope may be  
value. Certain countries consider electri  
[ups.com/ImportExport](http://ups.com/ImportExport) to verify if your ship.

• To qualify for the Letter rate, the UPS Express Envelope must v  
UPS Express Envelopes weighing more than 8 oz. will be billed  
Note: Express Envelopes are not recommended for shipments c  
containing sensitive personal information or breakable items. I  
or cash equivalent.

US 5090  
12-57-W87019961  
022X - 1032  
P. BROWN S. BGR  
DES MOINES IA 50319-0106  
IOWA ATTORNEY GENERAL  
1305 E WALNUT ST  
JAN 19 2017  
9564  
9564  
1030  
A  
L: BXA  
0  
one  
sifted

PATRICK HAGGERTY 5139293400 BAKER HOSTETTLER LLP 312 WALNUT ST CINCINNATI OH 45202		0.0 LBS LTR	1 OF 1
SHIP TO: OFFICE OF 5152815926 IOWA ATTORNEY GENERAL 1305 E. WALNUT STREET CONSUMER PROTECTION DIVISION SECURITY BREACH NOTIFICATIONS DES MOINES IA 50319			
	IA 503 9-30 		
UPS NEXT DAY AIR		1	
TRACKING #: LZ P57 W87 01 9961 9564			
			
BILLING: P/P			
Reference No.1: 106332.000002-10038			
XIL 17.01.28		NV45 84.0A 01/2017	

# Window Envelope

Use this envelope with shipping documents printed from a laser  
or inkjet printer on plain paper.

FOLD on this line and place in shipping pouch with bar code and delivery address visible

