

July 5, 2017

Via email: DOJ-CPB@doj.nh.gov

Consumer Protection and Antitrust Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: *Kayser-Roth Corporation, Greensboro, NC – Notice of Breach of Customer Information*

Dear Sir or Madam:

We represent Kayser-Roth, Inc., (“Kayser-Roth”) and on its behalf, are writing to notify you of a third party’s data breach that has affected its customers. Kayser-Roth is located at 102 Corporate Center Blvd., Greensboro, NC 27408. Kayser-Roth owns two websites, Hue.com (“Hue”) and Nononses.com (“Nononsense”), which use software provided, owned, and operated by Aptos Inc., (“Aptos”) to process their online orders. From February 2016 through December 2016 Aptos experienced a data breach. During that entire period of time, Hue and Nononsense used Aptos as their third party vendor to process their online orders. As a result, Kayser-Roth customers who placed an order on Hue or Nononsense from February 2016 through December 2016 may have had their personal information compromised.

The data breach compromised Aptos’ digital commerce solution. Aptos’ digital commerce solution was formerly known as Shop Visible digital commerce application. Due to the breach, unauthorized users gained access to Kayser-Roth’s customers’ names, addresses, phone numbers, email addresses and payment card information as those customers made transactions on Aptos’ platforms. The unauthorized users also gained access to payment card data for inactive payment cards no longer in use. The unauthorized users did not gain access to any debit card PIN numbers, credit card CVV codes, or any other type of payment card access code or password for Kayser-Roth customers. Also, no social security numbers for Kayser-Roth customers were disclosed.

Aptos did not notify Kayser-Roth of Aptos’ breach until February 6, 2017. At that time Aptos informed Kayser-Roth that information from a total of 90,548 customers, of which 492 were New Hampshire residents, may have been improperly accessed. Aptos has worked with the FBI Cyber division and the U.S. Department of Justice to investigate Aptos’ data breach. Aptos received an official request from the FBI to delay disclosure to its clients for a minimum of 60

Office of the Attorney General

July 5, 2017

Page 2

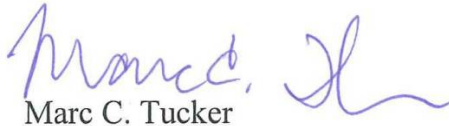
days while the FBI was conducting its investigation. Aptos complied with the FBI's official request to delay disclosure. Aptos also engaged the forensic cybersecurity firm Madiant to help stop and remove the malicious software that caused Aptos' data breach. The data breach has been remedied and Aptos has taken measures to prevent a data breach such as this one from occurring again. In addition, Kayser-Roth has notified all three major credit reporting agencies, Equifax, TransUnion, and Experian, of Aptos' breach.

We are attaching for your reference a copy of our customer notification letters. Kayser-Roth mailed a copy of the enclosed notices to potentially affected New Hampshire residents on June 26<sup>th</sup>, 2017. If you have any comments or concerns with respect to the attached letter, please contact me at your earliest convenience.

If you have any questions, please do not hesitate to contact me. My direct dial number is (919) 755-8713. Thank you for your assistance.

Very truly yours,

Smith Moore Leatherwood LLP

  
Marc C. Tucker

Enclosure



102 Corporate Center Boulevard Greensboro, NC 27408

June \_\_, 2017

[Name]

[Address]

Re: *Kayser-Roth Corporation, Greensboro, NC – Notice of Breach of Customer Information*

Dear Friends and Valued Customers:

No Nonsense, and our parent company Kayser-Roth, value the relationship we have with our customers. Consistent with that, we take the confidentiality of our customers' information very seriously and we work very hard to maintain it. That is why we regret that we are writing to notify you of an incident that may involve some of your information. Having said that, please know that we have NO reason to believe that it is sufficient information to have been used fraudulently – nor is there any evidence that it has been.

To give you the context, we use software provided by a third party vendor, Aptos Inc., to process Nononsense.com orders. Aptos is a highly experienced provider of retail technology and has a large universe of well-known brand customers. As has become increasingly common on the web in recent years, there was an intrusion into a portion of Aptos' systems that holds payment card data and certain other customer information for online orders placed on Nononsense.com. Specifically, this intrusion compromised the Aptos digital commerce solution we and many other brands use, and those responsible gained access to information, including names, addresses, phone numbers, email addresses and some payment card information as customers made transactions on Aptos' systems. They also gained access to historical payment card data for cards no longer in use.

We became aware of this intrusion to the Aptos system on February 6, 2017, and have since conducted our own review of the matter so we could provide all of the facts available at this time. **Aptos informed us that the breach lasted from February 2016, until December 6, 2016.** We believe that the information of 90,548 of our customers may have been compromised. **We are notifying you because our records indicate that you placed an order on [www.nononsense.com](http://www.nononsense.com) during that time period. Again, please know that Aptos is unaware of any incidents of fraud resulting from the breach, and there is no indication that the information that was accessed is usable for fraudulent purposes. Further, Aptos has informed us that they have stopped this intrusion.**

Aptos is continuing to take steps to protect you and the confidentiality of your information and to prevent any future incidents of this kind. Specifically, Aptos has worked with

the FBI Cyber division and the U.S. Department of Justice to investigate this incident. In connection with that, Aptos received an official request from the FBI to defer disclosure for a minimum of 60 days given the FBI's active investigation. In that time period, Aptos has worked with these agencies to supply the numbers of the affected payment cards to their issuers for monitoring.

Additionally and importantly, Aptos engaged Mandiant, a forensic cybersecurity firm, to assist with stopping and remedying the data security breach. As a result of their work, the malicious software used to access the system has been completely removed. Further, Aptos is in the process of deploying additional integrity monitoring software to alert it to any similar attack. And, with the assistance of external security consultants, Aptos has implemented changes to its systems for best-in-class security.

### **What should you do?**

We encourage you to take steps to protect yourself from any unauthorized use of your information and to remain vigilant regarding the possibility of identity theft or fraud – due to incidents like this and the many other cyber intrusions and breaches we have all read about in recent years. These steps include:

- Monitor your credit report on a regular basis and report any irregular activity to your bank or credit card company -- as major card companies have rules that restrict them from requiring you to pay for fraudulent charges that are reported in a timely manner;
- Update your password on your [www.nononsense.com](http://www.nononsense.com) accounts by logging into your account on Nononsense.com and selecting "Manage My Account." In step 1 "Account Information," you are able to click the link under "Password" to change your current password;
- Consider placing a fraud alert on your credit report. By doing this, any time someone tries to use your information to obtain credit, you will be contacted to verify the activity. You can add or remove a fraud alert at any time by contacting the three major credit reporting bureaus (Equifax, TransUnion, and Experian - contact information below).
- Periodically obtain credit reports from each nationwide credit reporting agency. If you discover a fraudulent transaction on your credit report, you should request that the reporting agency delete that information from your file; and
- Under federal law, you are entitled to a free copy of your credit report every 12 months from each of the three credit reporting agencies. You may obtain this report through [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228.
- In addition to the steps outlined above, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), call the FTC at 877-IDTHEFT (877-438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington DC 20580.



102 Corporate Center Boulevard Greensboro, NC 27408

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
(888) 766-0008 (fraud alert)	P.O. Box 4500	(800) 680-7289 (fraud alert)
Equifax Consumer Fraud Division	Allen, TX 75013	Fraud Victim Assistance Division
P.O. Box 740256	www.experian.com	P.O. Box 2000
Atlanta, GA 30374		Chester, PA 19016
www.equifax.com		www.transunion.com

On behalf of all of us at No Nonsense, please know that we care deeply about our customers and **we have established a dedicated, toll-free hotline to call for any questions about the information in this letter.** Specially trained representatives are available 9:00 am to 9:00 pm Eastern Time, Monday through Friday, at 1-844-512-9015.

Further, be assured that we will continue to implement improvements, including working closely with Aptos, to keep safe all personal information maintained on our website.

We are deeply grateful to our customers, and the safety and protection of your private information is one of our greatest concerns.

Sincerely,

---

Kevin Toomey  
President and CEO  
Kayser-Roth Corporation



102 Corporate Center Boulevard Greensboro, NC 27408

*IF YOU ARE AN IOWA RESIDENT:* You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
<http://www.iowaattorneygeneral.gov/>

*IF YOU ARE A MARYLAND RESIDENT:* You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
(410) 576-6574  
[Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

*IF YOU ARE AN OREGON RESIDENT:* You may obtain information about preventing identity theft from the FTC or the Oregon Attorney General's Office. These offices can be reached at:

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

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
(877) 877-9392 (toll-free in Oregon)  
(503) 378-4400  
[help@oregonconsumer.gov](mailto:help@oregonconsumer.gov)



102 Corporate Center Boulevard Greensboro, NC 27408

June \_\_, 2017

[Name]

[Address]

Re: *Kayser-Roth Corporation, Greensboro, NC – Notice of Breach of Customer Information*

Dear Friends and Valued Customers:

HUE, and our parent company Kayser-Roth, value the relationship we have with our customers. Consistent with that, we take the confidentiality of our customers' information very seriously and we work very hard to maintain it. That is why we regret that we are writing to notify you of an incident that may involve some of your information. Having said that, please know that we have NO reason to believe that it is sufficient information to have been used fraudulently – nor is there any evidence that it has been.

To give you the context, we use software provided by a third party vendor, Aptos Inc., to process Hue.com orders. Aptos is a highly experienced provider of retail technology and has a large universe of well-known brand customers. As has become increasingly common on the web in recent years, there was an intrusion into a portion of Aptos' systems that holds payment card data and certain other customer information for online orders placed on Hue.com. Specifically, this intrusion compromised the Aptos digital commerce solution we and many other brands use, and those responsible gained access to information, including names, addresses, phone numbers, email addresses and some payment card information as customers made transactions on Aptos' systems. They also gained access to historical payment card data for cards no longer in use.

We became aware of this intrusion to the Aptos system on February 6, 2017, and have since conducted our own review of the matter so we could provide all of the facts available at this time. **Aptos informed us that the breach lasted from February 2016 until December 6, 2016.** We believe that the information of 90,548 of our customers may have been compromised. **We are notifying you because our records indicate that you placed an order on [www.hue.com](http://www.hue.com) during that time period. Again, please know that Aptos is unaware of any incidents of fraud resulting from the breach, and there is no indication that the information that was accessed is usable for fraudulent purposes. Further, Aptos has informed us that they have stopped this intrusion.**

Aptos is continuing to take steps to protect you and the confidentiality of your information and to prevent any future incidents of this kind. Specifically, Aptos has worked with the FBI Cyber division and the U.S. Department of Justice to investigate this incident. In

connection with that, Aptos received an official request from the FBI to defer disclosure for a minimum of 60 days given the FBI's active investigation. In that time period, Aptos has worked with these agencies to supply the numbers of the affected payment cards to their issuers for monitoring.

Additionally and importantly, Aptos engaged Mandiant, a forensic cybersecurity firm, to assist with stopping and remedying the data security breach. As a result of their work, the malicious software used to access the system has been completely removed. Further, Aptos is in the process of deploying additional integrity monitoring software to alert it to any similar attack. And, with the assistance of external security consultants, Aptos has implemented changes to its systems for best-in-class security.

### **What should you do?**

We encourage you to take steps to protect yourself from any unauthorized use of your information and to remain vigilant regarding the possibility of identity theft or fraud – due to incidents like this and the many other cyber intrusions and breaches we have all read about in recent years. These steps include:

- Monitor your credit report on a regular basis and report any irregular activity to your bank or credit card company -- as major card companies have rules that restrict them from requiring you to pay for fraudulent charges that are reported in a timely manner;
- Update your password on your [www.hue.com](http://www.hue.com) account by logging into your account on Hue.com and selecting "Manage My Account." In step 1 "Account Information," you are able to click the link under "Password" to change your current password;
- Consider placing a fraud alert on your credit report. By doing this, any time someone tries to use your information to obtain credit, you will be contacted to verify the activity. You can add or remove a fraud alert at any time by contacting the three major credit reporting bureaus (Equifax, TransUnion, and Experian - contact information below).
- Periodically obtain credit reports from each nationwide credit reporting agency. If you discover a fraudulent transaction on your credit report, you should request that the reporting agency delete that information from your file; and
- Under federal law, you are entitled to a free copy of your credit report every 12 months from each of the three credit reporting agencies. You may obtain this report through [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228.
- In addition to the steps outlined above, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), call the FTC at 877-IDTHEFT (877-438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington DC 20580.





102 Corporate Center Boulevard Greensboro, NC 27408

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
(888) 766-0008 (fraud alert)	P.O. Box 4500	(800) 680-7289 (fraud alert)
Equifax Consumer Fraud Division	Allen, TX 75013	Fraud Victim Assistance Division
P.O. Box 740256	www.experian.com	P.O. Box 2000
Atlanta, GA 30374		Chester, PA 19016
www.equifax.com		www.transunion.com

On behalf of all of us at HUE, please know that we care deeply about our customers and **we have established a dedicated, toll-free hotline to call for any questions about the information in this letter.** Specially trained representatives are available 9:00 am to 9:00 pm Eastern Time, Monday through Friday, at 1-844-512-9015.

Further, be assured that we will continue to implement improvements, including working closely with Aptos, to keep safe all personal information maintained on our website.

We are deeply grateful to our customers, and the safety and protection of your private information is one of our greatest concerns.

Sincerely,

---

Kevin Toomey  
President and CEO  
Kayser-Roth Corporation



102 Corporate Center Boulevard Greensboro, NC 27408

*IF YOU ARE AN **IOWA** RESIDENT:* You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
<http://www.iowaattorneygeneral.gov/>

*IF YOU ARE A **MARYLAND** RESIDENT:* You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
(410) 576-6574  
[Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

*IF YOU ARE AN **OREGON** RESIDENT:* You may obtain information about preventing identity theft from the FTC or the Oregon Attorney General's Office. These offices can be reached at:

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

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
(877) 877-9392 (toll-free in Oregon)  
(503) 378-4400  
[help@oregonconsumer.gov](mailto:help@oregonconsumer.gov)