SMITHMOORE LEATHERWOOD
ATTORNEYS AT LAW

434 Fayetteville Street
Suite 2800
Raleigh, NC 27601

October 9, 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 July 1, 2017, through August 9, 2017, 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 July 1, 2017, through August 9, 2017, may have had their personal information compromised.

The data breach compromised Aptos' e-commerce solution. The intruder injected malicious code into Aptos' e-commerce platform. The intruder used the malicious code to encode and store payment card data when Kayser-Roth customers made transactions on Hue.com or Nononsense.com. Due to the breach, unauthorized users gained access to Kayser-Roth's customers' names, addresses, email addresses, and payment card information, including verification codes. It is Kayser-Roth's understanding that no social security numbers for Kayser-Roth customers were disclosed.

Aptos provided Kayser-Roth with information as to which customers were affected by the breach on September 21, 2017. Aptos has informed Kayser-Roth that information from a total of 6,488 customers, of which 31 were New Hampshire residents, may have been improperly accessed. Aptos has stated that it engaged a leading cybersecurity firm to help them determine the scope of the intrusion and put in place appropriate measures to strengthen its e-commerce platform. In addition, Aptos has notified the FBI of the breach. Aptos has informed Kayser-

SMITH MOORE LEATHERWOOD
ATTORNEYS AT LAW

Roth that it has no evidence that the breach is still ongoing. In addition, Kayser-Roth will notify all three major credit reporting agencies, Equifax, TransUnion, and Experian, of Aptos' breach.

We are attaching for your reference copies of our customer notification letters. It is our intention to mail a copy of the enclosed to affected individuals within the next five (5) business days. If you have any comments, questions, or concerns with respect to the attached letter, 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

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

<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<Address3>>
<<Address4>>
<<Address5>>
<<City>>, <<ST>> <<ZIP>>
<<Country>>

<<Date>>

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 a data breach that may involve some of your information.

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' system that holds payment card data and certain other customer information for online orders placed on Hue.com. Specifically, this data breach compromised Aptos' e-commerce platform that we and many other brands use, and those responsible gained access to names, addresses, email addresses and payment card information, including verification codes, as customers made transactions on Aptos' system.

Aptos provided Kayser-Roth with information as to which customers were affected by the data breach on September 21, 2017. We 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 July 1, 2017, until August 9, 2017.** We believe that the information of 6,488 of our customers may have been compromised. **We are notifying you because our records indicate that you placed an order on www.hue.com during that time period. Aptos has informed us that they have no evidence of further 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 engaged a leading cybersecurity firm to help them determine the scope of the intrusion and put in place appropriate measures to strengthen their e-commerce platform. Aptos' remediation efforts began immediately upon discovery of the data breach and they have no evidence that the intrusion is still ongoing. In addition, Aptos has notified the FBI of the data breach.

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 accounts 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 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, 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.

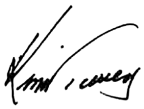
Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
(888) 766-0008 (fraud alert)	P.O. Box 4500	(800) 680-7289 (fraud alert)
Equifax Consumer Fraud Division	Allen, TX 75013	Fraud Victim Assistance Division
P.O. Box 740256	www.experian.com	P.O. Box 2000
Atlanta, GA 30374		Chester, 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 888-215-9697.

Further, be assured that we will continue to implement improvements and make changes we believe are necessary 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

*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 **NORTH CAROLINA** RESIDENT*: You may obtain information about preventing identity theft from the FTC or the North Carolina 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/

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

*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

*IF YOU ARE A **RHODE ISLAND** RESIDENT*: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

*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

Kayser-Roth Corporation

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

<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<Address3>>
<<Address4>>
<<Address 5>>
<<City>>, <<ST>> <<ZIP>>
<<Country>>

<<Date>>

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 a data breach that may involve some of your information.

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' system that holds payment card data and certain other customer information for online orders placed on Nononsense.com. Specifically, this data breach compromised Aptos' e-commerce platform that we and many other brands use, and those responsible gained access to names, addresses, email addresses and payment card information, including verification codes, as customers made transactions on Aptos' system.

Aptos provided Kayser-Roth with information as to which customers were affected by the data breach on September 21, 2017. We 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 July 6, 2017, until August 9, 2017.** We believe that the information of 6,488 of our customers may have been compromised. **We are notifying you because our records indicate that you placed an order on www.nononsense.com during that time period. Aptos has informed us that they have no evidence of further 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 engaged a leading cybersecurity firm to help them determine the scope of the intrusion and put in place appropriate measures to strengthen their e-commerce platform. Aptos' remediation efforts began immediately upon discovery of the data breach and they have no evidence that the intrusion is still ongoing. In addition, Aptos has notified the FBI of the data breach.

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 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 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, 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.

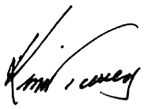
Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
(888) 766-0008 (fraud alert)	P.O. Box 4500	(800) 680-7289 (fraud alert)
Equifax Consumer Fraud Division	Allen, TX 75013	Fraud Victim Assistance Division
P.O. Box 740256	www.experian.com	P.O. Box 2000
Atlanta, GA 30374		Chester, 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 888-215-9697.

Further, be assured that we will continue to implement improvements and make changes we believe are necessary 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

*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 **NORTH CAROLINA** RESIDENT*: You may obtain information about preventing identity theft from the FTC or the North Carolina 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/

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

*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

*IF YOU ARE A **RHODE ISLAND** RESIDENT*: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

*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