McDonald Hopkins

A business advisory and advocacy law firm®

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

February 24, 2017

VIA E-MAIL: consumer@iowa.gov

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Rod's Western Palace – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Rod's Western Palace ("Rod's"). I write to provide notification concerning an incident that may affect the security of personal information of six-hundred and nine (609) Iowa residents. Rod's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Rod's does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

After identifying suspicious activity within Rod's e-commerce site on February 8, 2017, Rod's immediately initiated an internal investigation and engaged external IT consultants to assist. By February 10, 2017, Rod's identified the malicious code, permanently removed it from the site, and took additional steps to prevent a similar intrusion.

Rod's has learned that certain customer credit and debit card information may have been obtained by an unauthorized party from Rod's payment portal when purchasing through its online store at *www.rods.com*, from October 11, 2016 through February 10, 2017. Rod's does not store card data on its website; this data was taken (scraped) during the transaction. Purchases through Rod's physical retail locations and call center were not impacted by this incident.

Based on Rod's investigation, the information potentially involved in this incident may have included residents' names, credit or debit card numbers, card expiration dates and CVV2/CVC2/CID/CVDs (security codes on the front or back of the card). Debit PIN numbers were not obtained during this incident.

We wanted to make you (and the affected residents) aware of the incident and explain the steps Rod's is taking to safeguard the residents against identity fraud. Rod's will provide the

Iowa residents with electronic notice of this incident commencing on February 24, 2017, in substantially the same form as the communication attached hereto. Rod's will advise the residents to remain vigilant in reviewing financial and credit card account statements for fraudulent or irregular activity. Rod's will provide dedicated call center support to answer questions. Rod's will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Since learning of the incident, Rod's has implemented enhanced security safeguards to protect from similar intrusions. Rod's is also conducting ongoing monitoring of its website and payment portal to ensure that they are secure and cleared of any malicious code.

In addition, we have notified law enforcement and have notified the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

DAP/kjb
Encl.

[redacted]

From: Rod's Western Palace <rods@rods.com>
Sent: Friday, February 24, 2017
To: [redacted]
Subject: Information About Your Account-USA

ROD'S
TRUE WESTERN LIVING
Clothing • Boots • Home • Tack

February 24, 2017

[redacted]

Rod's Customer Number: [redacted]

Dear [redacted]

At Rod's Western Palace, protecting the privacy and security of your personal information is a top priority. We value and respect your privacy, which is why we are writing to advise you about an incident involving our online store and some of your personal information, to share the steps we have undertaken since discovering the incident, and to provide guidance on what you can do to protect yourself.

What Happened?

After identifying suspicious activity within our e-commerce site on February 8, 2017, we immediately initiated an internal investigation and engaged external IT consultants to assist us. By February 10th, we identified the malicious code, permanently removed it from our site, and took additional steps to prevent a similar intrusion.

We have learned that certain customer credit and debit card information may have been obtained by an unauthorized party from our payment portal when purchasing through our online store at www.rods.com, from October 11, 2016 through February 10, 2017. We do not store card data on our website; this data was taken during the transaction. **Purchases through our physical retail locations and call center were not impacted by this incident.**

What Information Was Involved?

Based on our investigation, the information potentially involved in this incident may have included your name, credit or debit card number, card expiration date and CVV2/CVC2/CID/CVD (security code on the front or back of the card). Debit PIN numbers were not obtained during this incident.

What We Are Doing

Since learning of the incident, we have implemented enhanced security safeguards to protect from similar intrusions. We are also conducting ongoing monitoring of our website and payment portal to ensure that they are secure and cleared of any malicious code. In addition, we have notified law enforcement and have notified the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

You should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover typically provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you. Out of an abundance of caution, we also recommend changing the password you use to access *www.rods.com.*

As a reminder, never provide your personal information in response to electronic communications regarding

security incidents.

For More Information

Your trust is a top priority for Rod's, and we deeply regret the inconvenience this may cause. The privacy and protection of our customers' information is a matter we take very seriously and we constantly enhance our processes and systems. As a "thank you" for your understanding and patience during this time, we are providing you with a coupon code (THANKS20) worth 20% off your next order. This code will be valid for 90 days.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 844-774-7742. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. EST. The response line will also be available on Saturday, February 25th from 9 a.m. to 5 p.m. EST.

Rod's values your business, and we appreciate your patience and support as we work through this issue.

Sincerely,
Scott Hartle
Owner/President

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

You may place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax	Experian	TransUnion LLC
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security	TransUnion LLC Security Freeze
P.O. Box 740241	Freeze	P.O. Box 2000
Atlanta, GA 30348	P.O. Box 9954	Chester, PA 19022
https://www.freeze.equifax.com	Allen, TX 75013	https://www.transunion.com/securityfreeze
1-800-685-1111	https://experian.com/freeze	1-888-909-8872
	1-888-397-3742	

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC and your state attorney general about fraud alerts and

security freezes. Instances of known or suspected identity theft should also be reported to law enforcement.

Iowa Residents: Office of the Attorney General, Consumer Protection Division, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164
Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.
Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.
North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.
Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392
Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

Rod's Western Palace
3099 Silver Drive, Columbus OH 43224 | (866) 326-1975 | rods@rods.com