Ryan Loughlin, Esquire
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 300
Wayne, PA 19087

April 7, 2017

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incidents

Dear Mr. Foster:

We represent One World Distribution, Inc. d/b/a One World Direct, 10 First Avenue East, Mobridge, SD 57601 ("OWD"), and are writing to notify you on behalf of Gildan, USA ("Gildan") of two data security incidents that may affect the security of payment card information of certain New Hampshire residents. The investigation into these incidents is ongoing and will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, neither OWD nor Gildan waives any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Cyber Security Incidents

OWD hosts and operates gildanonline.com on behalf of Gildan. On February 15, 2017, OWD received a report of suspicious activity on a card used legitimately at www.gildanonline.com. OWD began to investigate this report to determine what happened and if any other data may be impacted. Based upon this investigation, OWD determined that malware was inserted into the website on or about August 27, 2016, using a then unknown vulnerability in the e-commerce platform. OWD took the website down on February 15, 2017, immediately after discovering the malware, so that they could investigate further. Through a review of the malware, OWD determined that the malware was capable of collecting information provided by customers on the checkout page of the website. The information collected, between August 27, 2016 and February 15, 2017, included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If the customer was a registered user at the Gildan website, the customer's login and password would also have been collected.

During this investigation, OWD also learned that a file on www.gildanonline.com containing certain customer information from January 30, 2013 to March 19, 2014 was publicly accessible and was downloaded by unauthorized users. Although the credit card numbers and passwords in this file were encrypted, the investigation further determined that the decryption key was also located in the file and potentially could be discovered by someone with knowledge of what to look for.

OWD has no evidence confirming that illegal use of any personal information has occurred or that any material harm will result to any customer as a result of these incidents, although some customers who were exposed to the more recent malware incident have reported fraudulent charges on their payment cards.

Notice to New Hampshire Residents

On April 7, 2017, OWD, on behalf of Gildan, will begin mailing notice letters to New Hampshire customers who may be impacted by either incident. With respect to those who may be impacted by the malware, notice will be provided to approximately sixteen (16) New Hampshire residents. Notice of the malware is being provided in substantially the same form as the letter attached hereto as ***Exhibit A.*** With respect to those whose information was contained in the encrypted file, notice will be provided to approximately twenty-five (25) New Hampshire residents. Notice of the encrypted file is being provided in substantially the same form as the letter attached hereto as ***Exhibit B***.

Other Steps Taken

OWD immediately took the affected website offline so that credit and debit cards used to purchase products from www.gildanonline.com after February 15, 2017 are not at risk. OWD worked with Gildan to restore the website in a secure manner. OWD is also taking steps to further enhance the security of its systems to better protect against future incidents of this kind.

Additionally, OWD is providing potentially affected individuals with a free one year membership to Experian's IdentityWorks product. OWD is also providing potentially affected individuals with information on how to protect against identity theft and fraud, including a recommendation to review credit card statements for any suspicious activity, information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, OWD is providing written notice of this incident to other state regulators and consumer reporting agencies, where required.

Contact Information

Should you have any questions regarding this notification or other aspects of this incident, please contact me at (267) 930-4786.

Very Truly Yours,

Ryan Loughlin of
MULLEN COUGHLIN LLC

Enclosure

Exhibit A

[One World Direct Letterhead]

[DATE]

[Name]
[Street Address]
[City], [State] [Zip Code]

RE: Notice of Data Breach

Dear [Recipient Name]:

One World Distribution, Inc. d/b/a One World Direct ("OWD") is writing regarding a recent data security incident that may impact certain payment card and demographic information used by you at the e-commerce website, www.gildanonline.com, between August 27, 2016, and February 15, 2017. OWD is providing this notice on behalf of Gildan because OWD hosts and operates gildanonline.com. Both Gildan and OWD take the security of your information seriously, and we wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On February 15, 2017, OWD received a report of suspicious activity on a card used legitimately at www.gildanonline.com. We investigated this report to determine what happened and whether any other data may be impacted. Based upon this investigation, OWD determined that malware was inserted into the website on or about August 27, 2016, using a then unknown vulnerability in the e-commerce platform. We took the website down on February 15, 2017, immediately after discovering the malware, so that we could investigate further. Through a review of the malware, OWD determined that the malware was capable of collecting information provided by customers on the checkout page of the website. Although we have no evidence confirming that illegal use of any personal information has occurred or that any material harm will result to any customer as a result of this incident, some customers have reported fraudulent charges on their payment cards during the period noted above. Therefore, we want to alert you of this risk and inform you of actions that you can take to help protect against identity theft.

What Information Was Involved? Our investigation has revealed that the malware was capable of collecting demographic and credit card information entered on the website's checkout page between August 27, 2016, and February 15, 2017. The accessible customer information included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at www.gildanonline.com, your login and password would also have been accessible.

What We Are Doing. We have taken the website offline and worked with Gildan to restore the website in a secure manner. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators and consumer reporting agencies about this incident.

What You Can Do. You can stay vigilant by reviewing your credit card statements for any suspicious charges. In addition:

- Use good judgment in not responding to emails or other inquiries by those posing as a financial institution or other entities seeking your personal information.

- Carefully review all account statements and, if anything seems suspicious, place a fraud alert on your credit file. A fraud alert tells creditors to contact you before opening any new accounts or changing your existing accounts.

- Check your credit reports periodically. Victim information sometimes is held for use or shared among

a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

- If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and password.

You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

You also are offered assistance at no charge to you through Experian. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).Please note that this offer is available to you for one-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

In addition, while Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks SM as a complimentary one-year membership. This product provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 6/30/2017 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/identityone
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, please contact Experian's customer care team at 877-890-9332 by 6/30/2017. Be prepared to provide engagement number DB01251 as proof of eligibility for the identity restoration services by Experian. Additional information on the Experian IdentityWorks SM is enclosed.

For More Information. We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, or to inquire about what information OWD maintains about you, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at 1-800-741-6865, Monday through Friday, 7:00 a.m. to 9:00 p.m. CDT (excluding U.S. holidays).

Sincerely,

[Signature]

Thomas Unterseher
Co-Founder and CEO
One World Direct

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also 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. Note, however, that 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 agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 (NY residents please call 1-800-349-9960) www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19022-2000 1-888-909-8872 www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **Maryland** residents may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina** residents may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should be reported to law enforcement. This notice has not been delayed by law enforcement. If you provided an Armed Forces address, please contact us as soon as possible to provide us with your legal residence as your state's notice requirements may differ from the information provided to you above.

Exhibit B

[One World Direct Letterhead]

[DATE]

[Name]
[Street Address]
[City], [State] [Zip Code]

RE: Notice of Data Breach

Dear [Recipient Name]:

One World Distribution, Inc. d/b/a One World Direct ("OWD") is writing regarding a recent data security incident that may impact certain payment card and demographic information used by you at the e-commerce website, www.gildanonline.com sometime between January 30, 2013 and March 19, 2014. OWD is providing this notice on behalf of Gildan because OWD hosts and operates gildanonline.com. Both Gildan and OWD take the security of your information seriously, and we wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? We recently learned that a file on www.gildanonline.com containing certain customer information from January 30, 2013 to March 19, 2014 was publicly accessible and was downloaded by unauthorized users. Although the credit card numbers and passwords in the file were encrypted, the investigation further determined that the decryption key was also located in the file and potentially could be discovered by someone with knowledge of what to look for. We have no evidence confirming that illegal use of any personal information has occurred or that any material harm will result to any customer as a result of this incident, but we still wanted to alert you of this discovery and inform you of actions that you can take to help protect against identity theft.

What Information Was Involved? Our investigation revealed that the accessible file contained customer names, addresses, email addresses, telephone numbers, encrypted credit card numbers, and for some consumers an encrypted password for the website. The file *did not* contain credit card CVV numbers or expiration dates.

What We Are Doing. We took the website offline and worked with Gildan to restore the website in a secure manner. The website has been restored and it no longer contains this file. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators and consumer reporting agencies about this incident.

What You Can Do. You can stay vigilant by reviewing your credit card statements for any suspicious charges. In addition:

- Use good judgment in not responding to emails or other inquiries by those posing as a financial institution or other entities seeking your personal information.

- Carefully review all account statements and, if anything seems suspicious, place a fraud alert on your credit file. A fraud alert tells creditors to contact you before opening any new accounts or changing your existing accounts.

- Check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

- If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and password.

You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this offer is available to you for one-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks SM as a complimentary one-year membership. This product provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 6/30/2017 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/identityone
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, please contact Experian's customer care team at 877-890-9332 by 6/30/2017. Be prepared to provide engagement number DB01251 as proof of eligibility for the identity restoration services by Experian.

Additional information on the Experian IdentityWorks SM is enclosed.

For More Information. We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, or to inquire about what information OWD maintains about you, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at 1-800-741-6865, Monday through Friday, 7:00 a.m. to 9:00 p.m. CDT (excluding U.S. holidays).

Sincerely,

[Signature]

Thomas Unterseher
Co-Founder and CEO
One World Direct

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also 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. Note, however, that 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 agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay,

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 (NY residents please call 1-800-349-9960) www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19022-2000 1-888-909-8872 www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **Maryland** residents may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina** residents may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should be reported to law enforcement. This notice has not been delayed by law enforcement. An Armed Forces address does not indicate a military member's legal place of residence. If you provided an Armed Forces address, please contact us as soon as possible to provide us with your legal residence as your state's notice requirements may differ from the information provided to you above.