MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN
ATTORNEYS-AT-LAW WWW.MARSHALLDENNEHEY.COM
A PROFESSIONAL CORPORATION
2000 Market Street, Suite 2300 · Philadelphia, PA 19103
(215) 575-2600 · Fax (215) 575-0856

PENNSYLVANIA
Allentown
Doylestown
Erie
Harrisburg
King of Prussia
Philadelphia
Pittsburgh
Scranton
NEW JERSEY
Cherry Hill
Roseland
DELAWARE
Wilmington
OHIO
Cincinnati
Cleveland
FLORIDA
Ft. Lauderdale
Jacksonville
Orlando
Tampa
NEW YORK
Long Island
New York City
Westchester

Direct Dial: 215-575-2615
Email: djshannon@mdwcg.com

August 30, 2018

Via Email: attorneygeneral@doj.nh.gov
Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: **Dutch Gardens USA**
Our File No. 41105.00124

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are writing to notify you of a data security incident involving 130 New Hampshire residents. We are submitting this notification on behalf of our client, Richard Owen Nursery, Inc. d/b/a Dutch Gardens USA ("Dutch Gardens").

Nature Of The Security Breach

Dutch Gardens is a producer and distributor of home gardening products based in Bloomington, Illinois. On or about August 6, 2018, Dutch Gardens became aware that its website had become infected with malware. Dutch Gardens has determined that its website may have been infected during the period of September 29, 2017 until July 31, 2018. As a result, some of the personal information belonging to New Hampshire residents may have been exposed to others, including their first and last names, addresses used, credit card information, email addresses and phone numbers.

The residents involved in this incident will be forwarded letters notifying them of this incident on September 5, 2018. A copy of the form letter is attached hereto.

Steps Taken Relating To The Incident

Upon learning of the cyber-attack, Dutch Gardens took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter to determine how this incident occurred and who was impacted. Dutch Gardens conducted an analysis and remediation of its system to ensure that it is now secure. It is also in the process of reviewing internal policies and data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring in the future.

Should you need additional information regarding this matter, please contact me.

Very truly yours,

D.S.

DAVID J. SHANNON

DJS:jl
Encl.

Company Logo

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

The privacy and protection of our customers' personal information is a matter that we take very seriously. We are writing to inform you of a potential data breach at Dutch Gardens USA ("Dutch Gardens") that may have involved some of your personal information. Although a breach of information has not been confirmed, in the best interests of our customers, and in an abundance of caution and security, we believed it was necessary to take prudent precautions and to notify you of this incident.

What Happened
On or about August 6, 2018, Dutch Gardens became aware that its website had become infected with malware resulting in the potential compromise of some of its customers' personal information, including yours. Dutch Gardens has determined that its website may have been infected during the period of September 29, 2017 until July 31, 2018.

What Information Was Involved
Based on our investigation of this matter, we have determined that the personal information that may have been compromised included first and last names, addresses used, credit card information, email addresses and phone numbers.

What We Are Doing
Upon discovering this issue, we immediately conducted an investigation to determine how this incident occurred and who was impacted. We conducted an analysis and remediation of our system to ensure that it is now secure. We are also in the process of reviewing our internal policies and data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring in the future.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact our customer service department at 1-800-944-2250.

Sincerely,

Maarten van den Nouland

Maarten van den Nouland
Directeur, Dutch Gardens

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, *including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC").* You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate

documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.