Locke Lord LLP

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 PM 12: 05

20 Church Street
Hartford, CT 06103
Telephone: 860-525-5065
Fax: 860-527-4198
www.lockelord.com

Theodore P. Augustinos
Partner
Direct Telephone: 860-541-7710
Direct Fax: 888-325-9082
ted.augustinos@lockelord.com

March 23, 2017

Via Electronic Mail:
DOJ-CPB@doj.nh.gov

Via U.S. Mail:

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

Re: Veolia North America
Notification of Security Breach pursuant to N.H. Rev. Stat. § 359-C:20, "New Hampshire Right to Privacy Act."

To Whom it May Concern:

On behalf of our client, Veolia North America, an environmental solutions company (the "Company"), we hereby inform you of an incident arising from attack on a third-party shared server that hosts various websites that the Company utilizes to service customers that affected the personal information of five (5) New Hampshire residents.

Description of the Incident. On January 26, 2017, the third-party provider hosting the server (the "Host") was notified of malicious activity on the server by the attacker. The Host immediately notified the Company that its websites hosted on the server were impacted by this incident. The Host informed the Company that the intruder gained access to the server through an exploited file on another company's website that is also hosted on the server by the Host. Veolia investigated its website database to determine which of its customers were affected and what types of information were involved. Veolia determined that the intruder did in fact gain access and download certain customer and order related information, including an individual's first and last name, company name, address, email address, username and password for the individual's account on Veolia's website, and order history maintained on the website. With respect to the order history, for certain individuals, a full payment card number and expiration date were exposed to the attacker, while for other individuals, only the last four digits of a payment card and expiration date were exposed. The

full payment card numbers of five (5) New Hampshire residents were exposed in this incident. However, all of the full payment card numbers had an expiration date prior to January 26, 2017, and were therefore expired before the date of the attack.

Communication with Affected New Hampshire Residents. The affected New Hampshire residents are to be notified using the notification template enclosed with this letter as Exhibit A. Exhibit A-1 is the template for notifying the five (5) New Hampshire residents whose full payment card number was exposed. In addition, partial payment card numbers of twenty-nine (29) New Hampshire residents were also exposed, and the Company has elected to provide notification of the incident to those individuals as well. Exhibit A-2 is to be used to notify individuals where only the last four digits were exposed. The notification letters to the affected New Hampshire residents will be sent by First Class Mail on or about March 24, 2017.

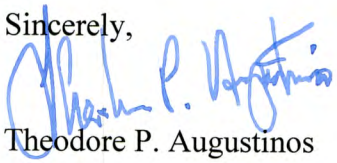
Steps Taken Following the Incident. Immediately after learning of this incident, the Company took down its servers and related websites until additional security measures were implemented. The Company's websites were restored on Monday March 6, 2017 with upgraded security, including the requirement for all users to reset passwords and to use stronger passwords. Also immediately after the Company learned of this incident, the Company investigated its website database to determine which of its customers were affected by the incident, and what types of their information was compromised.

The Host has reported this incident to appropriate legal authorities to investigate and prosecute the malicious intruder. We understand that the investigation by legal authorities is ongoing.

* * * * *

We trust that this letter and its enclosure provide you with the information required to assess this incident and the Company's response. Please let us know if you have any questions or if we may be of further assistance.

Sincerely,



Theodore P. Augustinos

Enclosure

Exhibit A-1

RECYCLEPAK

Veolia ES Technical Solutions, LLC
RecyclePaK Administrator
215 South Park Street
Port Washington, WI 53074

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 PM 12: 06

March 24, 2017

##C6749-L01-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE
COMPANY ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Incident involving your MERCHANT payment card ending in XXXX, with expiration date XX/XX

Dear Sample A Sample

Veolia is fully committed to protecting the privacy and personal information of our customers. Unfortunately, we are writing to inform you of an attack on a third-party shared server that hosts various websites that Veolia utilizes to service customers purchasing RecyclePak® prepaid recycling containers or requesting training through our Seminars website (the "Server"). The attack on the Server exposed your personal information to unauthorized access and acquisition by the attacker. While we are not aware of any misuse of any of the information involved in this incident, we apologize for any concern or inconvenience this incident may cause you. This letter provides information concerning this incident and the steps that have been taken to mitigate the risks to our customers, as well as guidance you may use to protect yourself.

What Happened

On January 26, 2017, our third-party provider hosting the Server (the "Host") was notified of malicious activity on the Server by the attacker. The Host immediately notified us that our websites hosted on the Server were impacted by this incident. The Host informed us that the intruder gained access to the Server through an exploited file on another company's website that is also hosted on the Server by the Host.

The Host reported the incident to law enforcement, which is investigating the matter and pursuing the attacker. The Host also had the stolen information deleted from the website where the attacker had posted it.

Veolia investigated its website database to determine which of our customers information where affected and what types of information were involved.

What Information Was Involved?

Our internal investigation of the incident confirmed that the intruder did in fact gain access and download certain customer and order related information. This information may include your first and last name, company name, address, email address, username and password for your account on our website, and order history maintained on the website.

0123456

Years ago, the Host was instructed by Veolia to obtain PCI DSS certification.[1] Unfortunately, prior to the PCI DSS certification (pre-2008), you may have made purchases on one of our websites whereby the full payment card number and expiration date were exposed to the attacker. Fortunately, the obtained payment card had an expiration date prior to the date of the attack (i.e., the card expired before January 26, 2017). The merchant, last four (4) digits of your card and expiration date are shown above.

We note that your payment card number referenced above may no longer be valid, and your account may have been closed since we collected this information from you at least eight years ago. Nevertheless, due to the exposure of the other information described above, and in the event your payment card account referenced above remains open, we are notifying you of this incident and encouraging you to review your account statements carefully to guard against fraudulent charges that may have occurred since January 26, 2017, or that may occur in the future.

How Did We Respond

Immediately after learning of this incident, we took down our servers and related websites until additional security measures were implemented. Our websites were restored on Monday March 6, 2017 with upgraded security, including the requirement for all users to reset passwords and to use stronger passwords. Also immediately after we learned of this incident, we investigated our website database to determine which of our customers were affected by the incident, and what types of their information was compromised.

The Host has reported this incident to appropriate legal authorities to investigate and prosecute the malicious intruder. We understand that the investigation by legal authorities is ongoing.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring 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 please visit www.annualcreditreport.com or call (toll free) 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Also enclosed is additional guidance for your protection, and disclosures applicable to residents of particular states.

Again, we apologize for any concern or inconvenience caused by this incident. We are fully committed to protecting your information. Please do not hesitate to contact us with any of your questions or concerns related to this incident by email at **na.information.security@veolia.com** or by calling our dedicated assistance line at **(877) 216-3862**, Monday through Friday, 9a.m. to 7p.m. EST (closed on U.S. observed holidays) and provide reference number **9404030817**.

Sincerely yours,

Robert Cappadona
Senior Vice-President, Industrial Business

Kevin Shaver
General Manager, Industrial Business

[1]The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard required to be implemented by organizations that handle branded credit cards (including Visa, MasterCard, American Express, Discover, and JCB).

ADDITIONAL GUIDANCE AND DISCLOSURES FOR RESIDENTS OF CERTAIN STATES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below. The following is contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Order your Free Credit Report. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

You can order your annual free credit report at www.annualcreditreport.com or by calling toll free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, which you can obtain from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov), to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Note that thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Notice for residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain these additional report(s).

Fraud Alert. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You also may want to consider contacting the major credit bureaus at the telephone numbers, websites, or addresses above to add a security freeze to your credit file. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. When adding a security freeze to your credit file, you must provide the following information (and the same information for your spouse if you are also requesting a security freeze for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Your request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

0123456

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. Contact information is provided below for the FTC and above for the consumer reporting agencies.

Notice for Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Notice for Rhode Island residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $10.

Contact the Federal Trade Commission and the Office of your State Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

Notice for North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Notice for Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Notice for Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

Notice for Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Notice for Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

Veolia ES Technical Solutions, LLC
RecyclePaK Administrator
215 South Park Street
Port Washington, WI 53074

March 24, 2017

##C6749-L01-0123456 0001 00000001 **********9-OELZZ 123
TO THE ESTATE OF SAMPLE A SAMPLE
COMPANY ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Incident involving your MERCHANT payment card ending in XXXX, with expiration date XX/XX

To the Estate of Sample A Sample

Veolia is fully committed to protecting the privacy and personal information of our customers. Unfortunately, we are writing to inform you of an attack on a third-party shared server that hosts various websites that Veolia utilizes to service customers purchasing RecyclePak® prepaid recycling containers or requesting training through our Seminars website (the "Server"). The attack on the Server exposed your personal information to unauthorized access and acquisition by the attacker. While we are not aware of any misuse of any of the information involved in this incident, we apologize for any concern or inconvenience this incident may cause you. This letter provides information concerning this incident and the steps that have been taken to mitigate the risks to our customers, as well as guidance you may use to protect yourself.

What Happened

On January 26, 2017, our third-party provider hosting the Server (the "Host") was notified of malicious activity on the Server by the attacker. The Host immediately notified us that our websites hosted on the Server were impacted by this incident. The Host informed us that the intruder gained access to the Server through an exploited file on another company's website that is also hosted on the Server by the Host.

The Host reported the incident to law enforcement, which is investigating the matter and pursuing the attacker. The Host also had the stolen information deleted from the website where the attacker had posted it.

Veolia investigated its website database to determine which of our customers information where affected and what types of information were involved.

What Information Was Involved?

Our internal investigation of the incident confirmed that the intruder did in fact gain access and download certain customer and order related information. This information may include your first and last name, company name, address, email address, username and password for your account on our website, and order history maintained on the website.

0123456

Years ago, the Host was instructed by Veolia to obtain PCI DSS certification.[1] Unfortunately, prior to the PCI DSS certification (pre-2008), you may have made purchases on one of our websites whereby the full payment card number and expiration date were exposed to the attacker. Fortunately, the obtained payment card had an expiration date prior to the date of the attack (i.e., the card expired before January 26, 2017). The merchant, last four (4) digits of your card and expiration date are shown above.

We note that your payment card number referenced above may no longer be valid, and your account may have been closed since we collected this information from you at least eight years ago. Nevertheless, due to the exposure of the other information described above, and in the event your payment card account referenced above remains open, we are notifying you of this incident and encouraging you to review your account statements carefully to guard against fraudulent charges that may have occurred since January 26, 2017, or that may occur in the future.

How Did We Respond

Immediately after learning of this incident, we took down our servers and related websites until additional security measures were implemented. Our websites were restored on Monday March 6, 2017 with upgraded security, including the requirement for all users to reset passwords and to use stronger passwords. Also immediately after we learned of this incident, we investigated our website database to determine which of our customers were affected by the incident, and what types of their information was compromised.

The Host has reported this incident to appropriate legal authorities to investigate and prosecute the malicious intruder. We understand that the investigation by legal authorities is ongoing.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring 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 please visit www.annualcreditreport.com or call (toll free) 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Also enclosed is additional guidance for your protection, and disclosures applicable to residents of particular states.

Again, we apologize for any concern or inconvenience caused by this incident. We are fully committed to protecting your information. Please do not hesitate to contact us with any of your questions or concerns related to this incident by email at **na.information.security@veolia.com** or by calling our dedicated assistance line at **(877) 216-3862**, Monday through Friday, 9a.m. to 7p.m. EST (closed on U.S. observed holidays) and provide reference number **9404030817**.

Sincerely yours,

R Cappadona

Robert Cappadona
Senior Vice-President, Industrial Business

Kevin Shaver
General Manager, Industrial Business

[1]The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard required to be implemented by organizations that handle branded credit cards (including Visa, MasterCard, American Express, Discover, and JCB).

ADDITIONAL GUIDANCE AND DISCLOSURES FOR RESIDENTS OF CERTAIN STATES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below. The following is contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Order your Free Credit Report. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

You can order your annual free credit report at www.annualcreditreport.com or by calling toll free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, which you can obtain from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov), to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Note that thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Notice for residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain these additional report(s).

Fraud Alert. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You also may want to consider contacting the major credit bureaus at the telephone numbers, websites, or addresses above to add a security freeze to your credit file. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. When adding a security freeze to your credit file, you must provide the following information (and the same information for your spouse if you are also requesting a security freeze for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Your request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

0123456

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. Contact information is provided below for the FTC and above for the consumer reporting agencies.

Notice for Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Notice for Rhode Island residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $10.

Contact the Federal Trade Commission and the Office of your State Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

Notice for North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Notice for Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Notice for Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

Notice for Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Notice for Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

EXHIBIT A-2

RECYCLEPAK

Veolia ES Technical Solutions, LLC
RecyclePaK Administrator
215 South Park Street
Port Washington, WI 53074

STATE OF NH
DEPT OF JUSTICE
2017 MAR 27 PM 12: 06

March 24, 2017

##C6749-L02-0123456 0001 00000001 **********9-OELZZ 123
SAMPLE A SAMPLE
COMPANY ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Incident

Dear Sample A Sample

Veolia is fully committed to protecting the privacy and personal information of our customers. Unfortunately, we are writing to inform you of an attack on a third-party shared server that hosts various websites that Veolia utilizes to service customers purchasing RecyclePak® prepaid recycling containers or requesting training through our Seminars website (the "Server"). The attack on the Server exposed your personal information to unauthorized access and acquisition by the attacker. While we are not aware of any misuse of any of the information involved in this incident, we apologize for any concern or inconvenience this incident may cause you. This letter provides information concerning this incident and the steps that have been taken to mitigate the risks to our customers, as well as guidance you may use to protect yourself.

What Happened

On January 26, 2017, our third-party provider hosting the Server (the "Host") was notified of malicious activity on the Server by the attacker. The Host immediately notified us that our websites hosted on the Server were impacted by this incident. The Host informed us that the intruder gained access to the Server through an exploited file on another company's website that is also hosted on the Server by the Host.

The Host reported the incident to law enforcement, which is investigating the matter and pursuing the attacker. The Host also had the stolen information deleted from the website where the attacker had posted it.

Veolia investigated its website database to determine which of our customers information where affected and what types of information were involved.

What Information Was Involved?

Our internal investigation of the incident confirmed that the intruder did in fact gain access and download certain customer and order related information. This information may include your first and last name, company name, address, email address, username and password for your account on our website, and order history maintained on the website. Your information also included the last four digits of a payment card you used for your website account, and the expiration date for that card. Please note that your full payment card number and the associated card verification value (CVV) code were not exposed in this incident. Nevertheless, due to the exposure of the other information described above, we are notifying you of this incident and encouraging you to review your account statements carefully to guard against fraudulent charges that may have occurred since January 26, 2017, or that may occur in the future.

0123456

How Did We Respond

Immediately after learning of this incident, we took down our servers and related websites until additional security measures were implemented. Our websites were restored on Monday March 6, 2017 with upgraded security, including the requirement for all users to reset passwords and to use stronger passwords. Also immediately after we learned of this incident, we investigated our website database to determine which of our customers were affected by the incident, and what types of their information was compromised.

The Host has reported this incident to appropriate legal authorities to investigate and prosecute the malicious intruder. We understand that the investigation by legal authorities is ongoing.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring 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 please visit www.annualcreditreport.com or call (toll free) 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Also enclosed is additional guidance for your protection, and disclosures applicable to residents of particular states.

Again, we apologize for any concern or inconvenience caused by this incident. We are fully committed to protecting your information. Please do not hesitate to contact us with any of your questions or concerns related to this incident by email at **na.information.security@veolia.com** or by calling our dedicated assistance line at **(877) 216-3862**, Monday through Friday, 9a.m. to 7p.m. EST (closed on U.S. observed holidays) and provide reference number **9404030817**.

Sincerely yours,

R Cappadona

Robert Cappadona
Senior Vice-President, Industrial Business

Kevin Shaver
General Manager, Industrial Business

ADDITIONAL GUIDANCE AND DISCLOSURES FOR RESIDENTS OF CERTAIN STATES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below. The following is contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Order your Free Credit Report. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

You can order your annual free credit report at www.annualcreditreport.com or by calling toll free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, which you can obtain from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov), to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Note that thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Notice for residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain these additional report(s).

Fraud Alert. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You also may want to consider contacting the major credit bureaus at the telephone numbers, websites, or addresses above to add a security freeze to your credit file. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. When adding a security freeze to your credit file, you must provide the following information (and the same information for your spouse if you are also requesting a security freeze for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Your request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

0123456

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. Contact information is provided below for the FTC and above for the consumer reporting agencies.

Notice for Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Notice for Rhode Island residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $10.

Contact the Federal Trade Commission and the Office of your State Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

Notice for North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Notice for Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Notice for Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

Notice for Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Notice for Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

RECYCLEPAK

Veolia ES Technical Solutions, LLC
RecyclePaK Administrator
215 South Park Street
Port Washington, WI 53074

March 24, 2017

##C6749-L02-0123456 0001 00000001 **********9-OELZZ 123
TO THE ESTATE OF SAMPLE A SAMPLE
COMPANY ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Security Incident

To the Estate of Sample A Sample

Veolia is fully committed to protecting the privacy and personal information of our customers. Unfortunately, we are writing to inform you of an attack on a third-party shared server that hosts various websites that Veolia utilizes to service customers purchasing RecyclePak® prepaid recycling containers or requesting training through our Seminars website (the "Server"). The attack on the Server exposed your personal information to unauthorized access and acquisition by the attacker. While we are not aware of any misuse of any of the information involved in this incident, we apologize for any concern or inconvenience this incident may cause you. This letter provides information concerning this incident and the steps that have been taken to mitigate the risks to our customers, as well as guidance you may use to protect yourself.

What Happened

On January 26, 2017, our third-party provider hosting the Server (the "Host") was notified of malicious activity on the Server by the attacker. The Host immediately notified us that our websites hosted on the Server were impacted by this incident. The Host informed us that the intruder gained access to the Server through an exploited file on another company's website that is also hosted on the Server by the Host.

The Host reported the incident to law enforcement, which is investigating the matter and pursuing the attacker. The Host also had the stolen information deleted from the website where the attacker had posted it.

Veolia investigated its website database to determine which of our customers information where affected and what types of information were involved.

What Information Was Involved?

Our internal investigation of the incident confirmed that the intruder did in fact gain access and download certain customer and order related information. This information may include your first and last name, company name, address, email address, username and password for your account on our website, and order history maintained on the website. Your information also included the last four digits of a payment card you used for your website account, and the expiration date for that card. Please note that your full payment card number and the associated card verification value (CVV) code were not exposed in this incident. Nevertheless, due to the exposure of the other information described above, we are notifying you of this incident and encouraging you to review your account statements carefully to guard against fraudulent charges that may have occurred since January 26, 2017, or that may occur in the future.

0123456

How Did We Respond

Immediately after learning of this incident, we took down our servers and related websites until additional security measures were implemented. Our websites were restored on Monday March 6, 2017 with upgraded security, including the requirement for all users to reset passwords and to use stronger passwords. Also immediately after we learned of this incident, we investigated our website database to determine which of our customers were affected by the incident, and what types of their information was compromised.

The Host has reported this incident to appropriate legal authorities to investigate and prosecute the malicious intruder. We understand that the investigation by legal authorities is ongoing.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring 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 please visit www.annualcreditreport.com or call (toll free) 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Also enclosed is additional guidance for your protection, and disclosures applicable to residents of particular states.

Again, we apologize for any concern or inconvenience caused by this incident. We are fully committed to protecting your information. Please do not hesitate to contact us with any of your questions or concerns related to this incident by email at **na.information.security@veolia.com** or by calling our dedicated assistance line at **(877) 216-3862**, Monday through Friday, 9a.m. to 7p.m. EST (closed on U.S. observed holidays) and provide reference number **9404030817**.

Sincerely yours,

R Cappadona

Robert Cappadona
Senior Vice-President, Industrial Business

Kevin Shaver
General Manager, Industrial Business

ADDITIONAL GUIDANCE AND DISCLOSURES FOR RESIDENTS OF CERTAIN STATES:

Your taking steps to protect yourself may include contacting credit reporting agencies as further described below. The following is contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Order your Free Credit Report. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

You can order your annual free credit report at www.annualcreditreport.com or by calling toll free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, which you can obtain from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov), to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Note that thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Notice for residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain these additional report(s).

Fraud Alert. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. Note that a fraud alert in your file can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You also may want to consider contacting the major credit bureaus at the telephone numbers, websites, or addresses above to add a security freeze to your credit file. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. When adding a security freeze to your credit file, you must provide the following information (and the same information for your spouse if you are also requesting a security freeze for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

Your request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.) The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

0123456

You may obtain additional information about fraud alerts and security freezes from the Federal Trade Commission, or the consumer reporting agencies. Contact information is provided below for the FTC and above for the consumer reporting agencies.

Notice for Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Notice for Rhode Island residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $10.

Contact the Federal Trade Commission and the Office of your State Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

Notice for North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Notice for Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Notice for Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

Notice for Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Notice for Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.