edgepark® Medical Supplies

1810 Summit Commerce Park
Twinsburg, Ohio 44087
www.edgepark.com

January 10, 2014

NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Pursuant to New Hampshire's Right to Privacy Act, §359-C:1, we are writing to notify you of a data security event that involved our company, RGH Enterprises, Inc. d/b/a Edgepark Medical Supplies, located in Twinsburg, Ohio. The security event potentially affected 26 New Hampshire residents. The details of the security event and steps we have taken to mitigate the situation are below.

NATURE OF THE SECURITY EVENT

On December 12, 2013, our information technology team was alerted to a problem with the web server environment located in Twinsburg, Ohio. Following a forensic examination of this environment, it was determined that on March 9, 2013, the environment had been compromised by an unknown individual or individuals (the "Hackers") who exploited a problem with Coldfusion, the Adobe software used to operate our website. These Hackers used a flaw in the software to install malware that intercepted information entered by users on our website, including the login names and passwords for the online account section of the website. The malware was detected shortly after Symantec, our virus protection software provider, identified the software as malware in its virus definitions. Previously, the malware was not present in Symantec's virus definitions. Once detected, the malware was immediately removed and a forensic investigation commenced. The investigation discovered that the malware intercepted online account usernames and passwords and stored them in a file on our website, which was accessed and downloaded by the Hackers between March 9 and March 11, 2013. The file was not accessed after March 11, 2013.

We maintain policies and procedures to protect customer confidentiality and conform to HIPAA privacy, security and breach notification requirements. This event did not result from any failure to adhere to such policies and procedures, and occurred despite our use of one of the top virus protection vendors in the United States.

The forensic investigation determined that the malware intercepted the online account usernames and passwords of 26 New Hampshire residents. If the usernames and passwords were used to access these individuals' online accounts, the following information about these individuals would be visible: name; date of birth; phone number; shipping and billing addresses; email address; credit card issuer, expiration date, and the last 4 digits of that credit card number; Edgepark account number; primary physician; diagnosis; order history;

and health insurer. Importantly, social security numbers were not subject to unauthorized access.

Not all of the 26 accounts were compromised in the same manner. More specifically, 25 individuals had their username and password intercepted because they entered that information when logging into their online account between March 9 and March 11, 2013. Any information these individuals typed in their online account profiles during their visit to the website would also have been intercepted (the categories of account information that users may edit in their online account profiles is listed in the paragraph above). Out of these 25 individuals, 1 entered credit card information, which included the user's full credit card number and expiration date, but not the credit card security code. An additional individual was impacted indirectly, in that the Hackers obtained the online account username and password of the individual's nurse, who is able to access this individual's online account.

We have no evidence that the Hackers logged into any online account or utilized any of the information available through the online accounts, and we did not experience any unusual volume or other activity on the website. Nevertheless, we are notifying individuals of this event out of an abundance of caution.

AFFECTED NEW HAMPSHIRE RESIDENTS

On Monday January 13, 2013, we will be sending a notice via first class mail to each of the potentially affected New Hampshire residents (template copies are enclosed), encouraging them to take measures to help prevent and detect any misuse of their information (e.g. canceling their payment cards, monitoring statements, and how to place a fraud alert with the three major credit monitoring bureaus), providing them with information regarding identity theft prevention, as well as our toll free telephone number that they may call for further information and assistance. We are also offering individuals the opportunity to enroll in 12 months of identity protection under the AllClear ID identity protection network at no cost. Template copies of the three versions of the patient notification letters are attached as Exhibit A: (1) a version that will be sent to the 1 resident who potentially had his/her online account username and password and full credit card number accessed; (2) a version that will be sent to the 24 individuals who potentially had their online account usernames and passwords (but not their full credit card numbers) accessed; and (3) a version that will be sent to the 1 individual whose nurse potentially had his/her online account accessed.

STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

We have taken appropriate steps to help prevent such incidents from occurring in the future, including resetting account passwords and removing the malware. We are continually evaluating and modifying our practices and the practices of our service providers to enhance the security and privacy of the confidential and sensitive information entrusted to us.

CONTACT INFORMATION

If the Office of the Attorney General would like to discuss the incident further, you may contact me at: 330-425-0267.

Sincerely,

Steven Eisenberg
Vice President and General Counsel

Enclosures (3)

Exhibit A

TEMPLATE NOTIFICATION LETTERS

edgepark®
Medical Supplies

Processing Center · P.O. Box 3825 · Suwanee, GA 30024

January 13, 2014

John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample:

This letter is to notify you that the website of Edgepark Medical Supplies was improperly accessed, resulting in the unauthorized access of certain personal information related to your account. At this time, there is no indication that your personal information has been misused in any way.

Edgepark takes your privacy very seriously. Our systems are safeguarded by a number of technological security measures including, but not limited to, industry-standard anti-virus software. However, on December 12, 2013, using this software, we discovered that our web servers were subject to unauthorized access between March 9 and 11, 2013 as a result of malware (which is similar to a computer software virus) that was identified on our system. Unfortunately, our anti-virus software provider did not identify this particular malware issue until shortly before we were notified of the incident. Upon discovery, the malware was immediately removed. We promptly investigated the incident and discovered that the malware may have resulted in the unauthorized access to the "account information" section of our website for some of our patients.

What This Means To You

We believe that unauthorized persons had access to your Edgepark account username and password, **but not your full credit card number, any security code associated with your credit card or social security number**. This would have allowed them to view certain account information, including your: name; date of birth; phone number; shipping and billing addresses; email address; the last four digits of your credit card number, credit card issuer and expiration date; Edgepark account number; primary physician; diagnosis; order history; and health insurer. However, we did not identify any unusual patterns accessing online accounts, and have received no reports from customers that their account was improperly accessed.

We take the protection of your personal information very seriously and have taken steps to prevent a similar occurrence, including resetting your account password. As a preventative measure, and to help strengthen the integrity of your personal information, please review the information included on Attachment 1 regarding identity theft prevention and steps that you can take to protect yourself.

In addition, out of an abundance of caution, we have arranged for you to have the option to receive 12 months of identity protection under the AllClear ID identity protection network at no cost to you.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use the identity protection service - there is no action required on your part. If a problem arises, simply call 1-877-676-0368 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: You are also eligible to obtain credit monitoring services by signing up online at enroll.allclearid.com or by phone by calling 1-877-676-0368 and using the following redemption code: 9999999999.

01030000000

More information about the AllClear Secure services is available on Attachment 2.

The security of your personal information is extremely important to us, and we work hard to ensure we have processes that keep it safe. We sincerely apologize for this situation and any inconvenience it may have caused. If you have questions please call 1-877-676-0368.

Sincerely,

Cindy Sackett

Cindy Sackett
Vice President of Compliance and Privacy Officer

Attachment 1
Information about Identity Theft Prevention

Although we are not aware of any instances of identity theft or other misuse of your personal information, we advise you to remain vigilant and consider taking the following steps:

What Steps Can You Take to protect Yourself?

- *Order a Copy of Your Credit Reports.* We highly recommend that you periodically obtain your credit report from one or more of the national credit reporting bureaus. 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 contact the three national credit reporting bureaus directly at the toll-free numbers below to order a free credit report once per year.

  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 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

  You should review credit reports carefully for any sign of fraud, such as unfamiliar accounts or credit inquires, debts that you cannot explain, medical debt collection notices from health care providers, or other unusual activity that you did not initiate or do not recognize. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

- *Read the Explanation of Benefits (EOB) Statements From Medicare and other Insurers.* Read the EOBs that you receive from your insurers. Make sure the health care claims to your insurers match the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, contact your insurer immediately to report the problem.

- *Request Medical Records.* You may also want to request a copy of your medical records from your health care providers or billing records from Medicare or other insurers to identify any health care items or services that were not provided to you. 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 medical privacy.

- *Monitor Your Medical, Financial and other Accounts.* We recommend that you closely monitor your account statements from your health care providers and suppliers, financial institutions and other account holders and, if you notice any unauthorized activity, promptly contact the account holder.

- *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 seven 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 above.

- *Credit Freezes.* You may have the right to put a credit freeze, also known as a security freeze, on your credit file. A credit freeze, which is different than a fraud alert, prevents new credit from being 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 creditors 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. Consequently, 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. 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. Information for Massachusetts residents is included at the end of this letter.

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790, www.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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to CoaguChek and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the 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 Maryland residents. 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 North Carolina residents. You may also obtain information about preventing and avoiding identity theft from 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

Attachment 2
Terms of Use for AllClear Secure

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage;
- No cost to you - ever. AllClear Secure is paid for by Edgepark Medical Supplies.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur;
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud; and
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

edgepark®
Medical Supplies
Processing Center · P.O. Box 3825 · Suwanee, GA 30024

January 13, 2014

John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample:

This letter is to notify you that the website of Edgepark Medical Supplies was improperly accessed, resulting in the unauthorized access of certain personal information related to your account. At this time, there is no indication that your personal information has been misused in any way.

Edgepark takes your privacy very seriously. Our systems are safeguarded by a number of technological security measures including, but not limited to, industry-standard anti-virus software. However, on December 11, 2013, using this software, we discovered that our web servers were subject to unauthorized access between March 9 and 11, 2013 as a result of malware (which is similar to a computer software virus) that was identified on our system. Unfortunately, our anti-virus software provider did not identify this particular malware issue until shortly before we were notified of the incident. Upon discovery, the malware was immediately removed. We promptly investigated the incident and discovered that the malware may have resulted in the unauthorized access to the "account information" section of our website for some of our patients.

What This Means To You

We believe that unauthorized persons had access to your Edgepark account username, password and your 16-digit credit card number, **but not any security code associated with your credit card or social security number**. Your Edgepark account username and password would have allowed them to access your online account and view certain account information, including your: name; date of birth; phone number; shipping and billing addresses; email address; credit card issuer and expiration date; Edgepark account number; primary physician; diagnosis; order history; and health insurer. However, we did not identify any unusual patterns accessing online accounts, and have received no reports from customers that their account was improperly accessed.

We take the protection of your personal information very seriously and have taken steps to prevent a similar occurrence, including resetting your account password. As a preventative measure, and to help strengthen the integrity of your personal information, please review the information included on Attachment 1 regarding identity theft prevention and steps that you can take to protect yourself.

In addition, out of an abundance of caution, we have arranged for you to have the option to receive 12 months of identity protection under the AllClear ID identity protection network at no cost to you.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use the identity protection service - there is no action required on your part. If a problem arises, simply call 1-877-676-0368 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: You are also eligible to obtain credit monitoring services by signing up online at enroll.allclearid.com or by phone by calling 1-877-676-0368 and using the following redemption code: 9999999999.

More information about the AllClear Secure services is available on Attachment 2.

The security of your personal information is extremely important to us, and we work hard to ensure we have processes that keep it safe. We sincerely apologize for this situation and any inconvenience it may have caused. If you have questions please call 1-877-676-0368.

Sincerely,

Cindy Sackett

Cindy Sackett
Vice President of Compliance and Privacy Officer

Attachment 1
Information about Identity Theft Prevention

Although we are not aware of any instances of identity theft or other misuse of your personal information, we advise you to remain vigilant and consider taking the following steps:

What Steps Can You Take to protect Yourself?

- *Order a Copy of Your Credit Reports.* We highly recommend that you periodically obtain your credit report from one or more of the national credit reporting bureaus. 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 contact the three national credit reporting bureaus directly at the toll-free numbers below to order a free credit report once per year.

  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 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

  You should review credit reports carefully for any sign of fraud, such as unfamiliar accounts or credit inquires, debts that you cannot explain, medical debt collection notices from health care providers, or other unusual activity that you did not initiate or do not recognize. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

- *Read the Explanation of Benefits (EOB) Statements From Medicare and other Insurers.* Read the EOBs that you receive from your insurers. Make sure the health care claims to your insurers match the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, contact your insurer immediately to report the problem.

- *Request Medical Records.* You may also want to request a copy of your medical records from your health care providers or billing records from Medicare or other insurers to identify any health care items or services that were not provided to you. 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 medical privacy.

- *Monitor Your Medical, Financial and other Accounts.* We recommend that you closely monitor your account statements from your health care providers and suppliers, financial institutions and other account holders and, if you notice any unauthorized activity, promptly contact the account holder.

- *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 seven 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 above.

- *Credit Freezes.* You may have the right to put a credit freeze, also known as a security freeze, on your credit file. A credit freeze, which is different than a fraud alert, prevents new credit from being 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 creditors 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. Consequently, 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. 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. Information for Massachusetts residents is included at the end of this letter.

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790, www.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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to CoaguChek and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the 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 Maryland residents. 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 North Carolina residents. You may also obtain information about preventing and avoiding identity theft from 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

Attachment 2
Terms of Use for AllClear Secure

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage;
- No cost to you - ever. AllClear Secure is paid for by Edgepark Medical Supplies.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur;
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud; and
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

edgepark®
Medical Supplies
Processing Center · P.O. Box 3825 · Suwanee, GA 30024

January 13, 2014

John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample:

This letter is to notify you that the website of Edgepark Medical Supplies was improperly accessed, resulting in the unauthorized access of certain personal information related to your account. At this time, there is no indication that your personal information has been misused in any way.

Edgepark takes your privacy very seriously. Our systems are safeguarded by a number of technological security measures including, but not limited to, industry-standard anti-virus software. However, on December 12, 2013, using this software, we discovered that our web servers were subject to unauthorized access between March 9 and 11, 2013 as a result of malware (which is similar to a computer software virus) that was identified on our system. Unfortunately, our anti-virus software provider did not identify this particular malware issue until shortly before we were notified of the incident. Upon discovery, the malware was immediately removed. We promptly investigated the incident and discovered that the malware may have resulted in the unauthorized access to the "account information" section of our website for some of our patients.

What This Means To You

We believe that unauthorized persons had access to the EdgePark account username and password of the nurse who is responsible for your account. With this information, they could have potentially signed into the nurse's EdgePark account, which would have potentially allowed them to access the accounts of customers for whom the nurse is responsible, including you. This would have allowed them to view certain account information, including your: name; date of birth; phone number; shipping and billing addresses; email address; the last four digits of your credit card number, credit card issuer and expiration date **(but not your full credit card number, any associated security code, or your social security code)**; Edgepark account number; primary physician; diagnosis; order history; and health insurer. However, we did not identify any unusual patterns accessing online accounts, and have received no reports from customers that their account was improperly accessed.

We take the protection of your personal information very seriously and have taken steps to prevent a similar occurrence, including resetting the nurse's account password. As a preventative measure, and to help strengthen the integrity of your personal information, please review the information included on Attachment 1 regarding identity theft prevention and steps that you can take to protect yourself.

In addition, out of an abundance of caution, we have arranged for you to have the option to receive 12 months of identity protection under the AllClear ID identity protection network at no cost to you.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use the identity protection service - there is no action required on your part. If a problem arises, simply call 1-877-676-0368 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: You are also eligible to obtain credit monitoring services by signing up online at enroll.allclearid.com or by phone by calling 1-877-676-0368 and using the following redemption code: 9999999999.

More information about the AllClear Secure services is available on Attachment 2.

The security of your personal information is extremely important to us, and we work hard to ensure we have processes that keep it safe. We sincerely apologize for this situation and any inconvenience it may have caused. If you have questions please call 1-877-676-0368.

Sincerely,

Cindy Sackett

Cindy Sackett
Vice President of Compliance and Privacy Officer

Attachment 1
Information about Identity Theft Prevention

Although we are not aware of any instances of identity theft or other misuse of your personal information, we advise you to remain vigilant and consider taking the following steps:

What Steps Can You Take to protect Yourself?

- *Order a Copy of Your Credit Reports.* We highly recommend that you periodically obtain your credit report from one or more of the national credit reporting bureaus. 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 contact the three national credit reporting bureaus directly at the toll-free numbers below to order a free credit report once per year.

  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 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

  You should review credit reports carefully for any sign of fraud, such as unfamiliar accounts or credit inquires, debts that you cannot explain, medical debt collection notices from health care providers, or other unusual activity that you did not initiate or do not recognize. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

- *Read the Explanation of Benefits (EOB) Statements From Medicare and other Insurers.* Read the EOBs that you receive from your insurers. Make sure the health care claims to your insurers match the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, contact your insurer immediately to report the problem.

- *Request Medical Records.* You may also want to request a copy of your medical records from your health care providers or billing records from Medicare or other insurers to identify any health care items or services that were not provided to you. 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 medical privacy.

- *Monitor Your Medical, Financial and other Accounts.* We recommend that you closely monitor your account statements from your health care providers and suppliers, financial institutions and other account holders and, if you notice any unauthorized activity, promptly contact the account holder.

- *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 seven 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 above.

- *Credit Freezes.* You may have the right to put a credit freeze, also known as a security freeze, on your credit file. A credit freeze, which is different than a fraud alert, prevents new credit from being 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 creditors 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. Consequently, 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. 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. Information for Massachusetts residents is included at the end of this letter.

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790, www.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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to CoaguChek and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the 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 Maryland residents. 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 North Carolina residents. You may also obtain information about preventing and avoiding identity theft from 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

Attachment 2
Terms of Use for AllClear Secure

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage;
- No cost to you - ever. AllClear Secure is paid for by Edgepark Medical Supplies.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur;
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud; and
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077