Interactive MedicalSystems
PO Box 1349
Wake Forest, NC 27588

February 14, 2020

F3244-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE -L01
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Re: ***Important Notice of Data Breach***
Plan Sponsor: COMPANY_NAME

We, Interactive Medical Systems Corporation or IMS, are a third-party administrator that was retained by your Plan Sponsor to perform administration of the flexible spending or health plan which it sponsors as an employer ("the Plan"). We value our business relationship with the Plan and we also greatly respect your privacy, which is why we are writing on behalf of the Plan to notify you concerning a data security breach that has resulted in the disclosure of certain personal information about you. Although we currently have no information that would indicate your personal information has been used in an unauthorized manner, we are writing to provide information about that incident and steps you can take to inform and protect yourself.

What Happened. We informed the Plan that on December 31, 2019, we received a technical alert concerning an email address of an IMS employee which indicated that the employee's email user account was restricted from sending messages. At that time, we suspected that the account had been compromised due to a phishing email. We immediately took steps to secure the user's email account and, though there was no indication other accounts were affected, all other email accounts within our company. We initiated an investigation to assess the incident's scope, including a review of all emails and attachments in the user's account during the compromised period and engaging a third-party cybersecurity firm to perform a comprehensive forensics investigation. There was no indication that your employer's systems or servers were involved. Our investigation has confirmed that emails within the affected user's email account between July 19 and December 31, 2019 were exposed to an unauthorized third party as a result of a sophisticated phishing attack. A "phishing" email is a malicious email that appears to be legitimate to entice the user into giving up login information. An example would be an email appearing to come from your own email system claiming that "Your mailbox is almost out of space and requires immediate attention to avoid disconnection." There would be a link in the email that appears to lead to your own email system login page, but instead takes you to an identical looking page hosted on a malicious server. By logging in, you are handing over your credentials to the malicious actor. Typically, the malicious login page would then redirect you to the legitimate login page in an effort to make you think you simply mistyped your password, avoiding suspicion. An automatic forwarding rule had been placed on the IMS employee email account which was immediately removed on discovery.

What Information Was Involved? Through our forensic investigation, we have determined that the categories of personal information exposed varies for each affected individual and may have included: **First and Last Name, Last Four Digits of Social Security Number, Transaction Date and Amount, Plan Sponsor/Employer Name, Address.** Your full Social Security Number was never compromised.

What We Are Doing. We want to assure you that we are taking steps to prevent a similar event from occurring in the future, and to otherwise protect the privacy and security of your information. These actions include optimizing network configuration for security, upgrading our email platform for enhanced monitoring and security, implementing multi-factor authentication for email access and electronic data storage systems, and adding a secondary anti-virus detection tool to our existing anti-virus detection tools, implementing stricter passwords and password management policies, enhancing email threat detection, branding email login pages and improving data privacy training and awareness.

What You Can Do. In addition to our efforts, we strongly advise that you take certain steps to minimize or eliminate potential harm. First, we recommend that you closely monitor your financial accounts. If you see any unauthorized activity, promptly contact your financial institution. Please also review the enclosed Additional Important Information for information that could pertain to you.

Below is a checklist of additional suggestions of how you can best protect yourself in this situation.

1. Regularly review your bank, credit card and debit card account statements and immediately report any suspicious activity to your bank or credit union.

2. Monitor your credit reports with the major credit reporting agencies:

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241, Atlanta, GA 30374-0241	P.O. Box 2104, Chester, PA 19022	P.O. Box 1000, Allen, TX 75013
www.equifax.com	www.experian.com	www.transunion.com

We recommend that you continue to monitor your credit regularly. You may contact the three U.S. credit reporting agencies to obtain a free credit report. The easiest way to do this is to request a free credit report at www.annualcreditreport.com.

Call the credit reporting agency at the telephone number on the report if you find:
- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address and social security number.

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and file a report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

4. You might also wish to place a fraud alert on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the numbers listed above to place fraud alerts with all of the agencies.

5. You may also consider placing a security freeze on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. You have the right to place a security freeze on your credit report free of charge. A security freeze may cause delay should you wish to obtain credit but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. You may also get information about security freezes by contacting the credit bureaus at the following addresses.

- **Equifax**: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- **Experian**: http://www.experian.com/consumer/security_freeze.html
- **TransUnion**: https://www.transunion.com/credit-freeze/place-credit-freeze

6. The identities of children should also be protected. You may wish to take the steps to protect your children's information suggested by the Federal Trade Commission. These steps include monitoring your children's credit reports and placing fraud alerts and security freezes on their credit reports as you would your own. More information on protecting children can be found at https://www.consumer.ftc.gov/articles/0040-child-identity-theft. You may contact the FTC at 877-438-4338 (toll-free) or 866-653-4261 (TTY)(toll-free).

7. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you remain vigilant and regularly check your credit report. Just call one of the numbers for the major credit monitoring services listed above to order your reports or to keep a fraud alert in place. Helpful information about fighting identity

theft, placing a security freeze, and obtaining a free copy of your credit report is available on the FTC website, which you may find at http://www.ftc.gov/bcp/edu/microsites/idtheft/. You may contact the FTC at the toll-free numbers above or by mailing written correspondence to 600 Pennsylvania Avenue, NW Washington, DC 20580, United States.

Please know that the protection and security of your personal information is our utmost priority, and we sincerely regret any inconvenience or concern that this matter may have caused. If you have any questions or concerns, you may contact us between the hours of 10 AM and 4 PM, Eastern Standard Time, at **833-315-0436**. We are here to assist in any way we can.

Best regards,

Interactive Medical Systems Corporation

Additional Important Information

For residents of All States, including Hawaii, Michigan, Missouri, North Carolina, Vermont Illinois, Iowa, Maryland, Oregon, West Virginia and Virginia: It is recommended or required that we notify you to remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit reports free of charge once every 12 months from each of the three nationwide credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at: https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland, New York, and North Carolina: You can obtain information from the Maryland, New York, and North Carolina Offices of the Attorneys General, the New York Department of State Division of Consumer Protection, and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General - Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
888-743-0023 or 410-528-8662
www.oag.state.md.us

North Carolina Office of the Attorney General – Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699
877-566-7226 or 919-716-6000
https://ncdoj.gov/

New York State Office of the Attorney General - The Capitol
Albany, NY 12224-0341
800-771-7755
https://ag.ny.gov

Federal Trade Commission Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
877-IDTHEFT (438-4338)
www.ftc.gov/faq/consumer-protection/report-identity-theft

New York Department of State Division of Consumer Protection
One Commerce Plaza, 99 Washington Ave., Albany, NY 12331-0001
800-697-1220, www.dos.ny.gov/consumerprotection

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Rhode Island: Pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze. This incident involves N/A Rhode Island residents. You may obtain information about avoiding identity theft at: Office of the State of Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903, 401-274-4400, www.riag.ri.gov.

For residents of New Mexico: The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.
For residents of Horry County South Carolina: To report a security breach or identity theft contact the Horry County Police (Desk Officer):
Conway Area: ML Brown Building, 2560 Main Street, Conway, SC 29526 (843) 915-8012.
South Strand: 9630 Scipio Lane, Myrtle Beach, SC 29588 (843) 915-7953
North Strand: 109 Highway 57 North, Little River SC 29566 (843) 915-5685
For residents of West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below:

Fraud Alerts: There are two types of fraud alerts 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 one year. 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 contacting any of the three national credit reporting agencies.

Credit Freeze: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number (PIN) that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc. (2) Social Security number (3) Date of birth (4) If you have moved in the past five years, provide the addresses where you have lived over the prior five years (5) Proof of current address such as a current utility bill or telephone bill (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.), and (7) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three

business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to Consumer Financial Protection Burea11, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit ''prescreened'' offers of credit and insurance you get based on information in your credit report.
- You have a right to place a ''security freeze'' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Mailing Address: The mailing address for Interactive Medical Systems Corporation is PO Box 1349, Wake Forest, NC 27588

For residents of All States:

Security Freeze: You also have the right to place a security freeze on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her 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. The 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 may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788 Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554 Allen, TX 75013
www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000 Chester, PA 19022
https://www.transunion.com/credit-freeze/place-credit-freeze

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 state. You can obtain information from these sources about fraud alerts and security freezes. You should also contact your local law

enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

More information can be obtained by contacting the Federal Trade Commission at:
Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.