Stradling
Attorneys at Law

STRADLING YOCCA CARLSON & RAUTH, P.C.
660 NEWPORT CENTER DRIVE, SUITE 1600
NEWPORT BEACH, CA 92660-6422
SYCR.COM

CALIFORNIA
NEWPORT BEACH
SACRAMENTO
SAN DIEGO
SAN FRANCISCO
SANTA BARBARA
SANTA MONICA
COLORADO
DENVER
NEVADA
RENO
WASHINGTON
SEATTLE

KATHLEEN M. MARCUS
949.725.4080
KMARCUS@SYCR.COM

STATE OF NH
DEPT OF JUSTICE
2016 MAR 10 PM 12:20

March 9, 2016

Via Facsimile and FEDEX
(603) 271-2110

The Honourable Kelly A. Ayotte
Attorney General of the State of New Hampshire
Department of Justice
33 Capitol Street
Concord, NH 03301
E-mail: attorneygeneral@doj.nh.gov

Dear Madam:

My firm, Stradling Yocca Carlson & Rauth, represents Endologix, Inc. We are contacting you because we have learned of a data security incident that involved personal information of New Hampshire residents.

Endologix was targeted by a fraudulent "phishing" email that appeared to come from an internal Endologix email address. This email was not recognized as fraudulent, and, consequently, Endologix unknowingly provided the 2015 W-2 forms of certain employees to an unauthorized third party. This matter involved an isolated e-mail attack; we do not believe that Endologix's systems were breached or that Endologix user accounts or login credentials were accessed.

Endologix will be sending notices to the affected New Hampshire residents this week. A copy of a sample notice is attached as Exhibit A. Endologix also notified law enforcement.

Endologix has offered two years of credit monitoring services to the affected employees. In addition, Endologix will be acting swiftly to implement additional preventative measures, including adopting new policies and procedures that will empower their personnel to better recognize a suspicious request, even from within Endologix, and enable them to verify the origin of a request prior to releasing sensitive information.

Please contact me if you have any questions or need further information.

Very truly yours,

Kathleen M. Marcus
STRADLING YOCCA CARLSON & RAUTH, P.C.

EXHIBIT A

3910 Brickway Blvd.

Santa Rosa, CA 95403

Endologix

March [XX], 2016

[Employee Name]
[Employee Address]
[Employee City, State Zip]

Important Security and Protection Notification
Please read this entire letter.

Dear [Employee Name]:

We are contacting you because we have learned of a data security incident that involved some of your personal information. Endologix was targeted by a fraudulent email phishing scam seeking employee tax documentation, and your W-2 form was disclosed in connection with that attack.

We recommend that you closely review the information provided in this letter for steps that you can take to protect yourself against potential misuse of your information.

What Happened?

On March 3, 2016, Endologix was targeted by a fraudulent "phishing" email that appeared to come from an internal Endologix email address. This email was not recognized as fraudulent, and, consequently, we unknowingly provided the 2015 W-2 forms of current and former TriVascular employees to an unauthorized third party. This matter involved an isolated e-mail attack; we do not believe that Endologix's systems were breached or that Endologix user accounts or login credentials were accessed.

The W-2 forms contained personal information, including name, address, social security number, and financial information. As indicated above, no other information beyond copies of the W-2 forms was provided in response to the fraudulent email.

What We Are Doing to Protect Your Information

The privacy and protection of our employees' information is a matter we take very seriously, and we have worked swiftly to investigate and resolve the incident. We have reported this incident to the Federal Bureau of Investigation, the Internal Revenue Service, and several state agencies. We intend to cooperate fully with any law enforcement inquiries regarding these events, but we have not delayed notice to you as a result of any potential government investigations. We also are taking additional measures within the company to strengthen our security.

Endologix will be acting swiftly to implement additional preventative measures, including adopting new policies and procedures that will empower our personnel to better recognize a suspicious request,

Endologix

even from within Endologix, and enable them to verify the origin of a request prior to releasing sensitive information.

For any employee whose information was exposed in this incident, Endologix is offering two years of free identity protection services from Experian, through the ProtectMyID® Elite program. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: June 30, 2016** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide the following engagement number: PC99854

For additional details regarding your ProtectMyID membership, please see the attachment.

Steps You Can Take

Please take additional preventive measures now to help prevent and detect any misuse of your information. It is important that you remain vigilant by reviewing your accounts statements and monitoring free credit reports. If you suspect incidents of identity theft or unusual activity on your accounts, be sure to report it immediately to your financial institutions or other relevant entities. In addition, you may contact the Federal Trade Commission (FTC), state attorney general, or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the Commission and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

In addition to committing identity theft, scammers frequently use W-2 forms to file fraudulent tax refund requests with the Internal Revenue Service and state tax authorities. It is recommended that you file your federal and state taxes as soon as possible so that scammers do not file a fraudulent return prior to your submission of your legitimate tax documentation. For additional information on how to protect

Endologix

yourself against tax-related identity theft or fraud please review the Identity Theft Information for Taypayers guide published by the IRS, which is available at https://www.irs.gov/pub/irs-pdf/p5027.pdf.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you should request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting bureaus to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

Endologix

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

We sincerely apologize for this incident, and we regret any inconvenience it may cause you. We encourage you to enroll in the ProtectMyID program and take any other appropriate protective steps as outlined in this letter. If you have any questions, please call me at (707) 543-8709 or Tonja Jennings at (707) 543-8634.

Sincerely,

Michael Kramer
COO – Endologix Santa Rosa

IF YOU ARE AN IOWA RESIDENT:
You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

Endologix

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

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

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

Endologix

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP WITH EXPERIAN:

- A credit card is not required for enrollment.
- Once your ProtectMyID membership is activated, you will receive the following features:
  - **Free copy of your Experian credit report**
  - **Surveillance Alerts for:**
    - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
    - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
    - **Change of Address:** Alerts of any changes in your mailing address.
  - **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
    - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
  - **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
  - **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.