

Endress+Hauser Inc., 2350 Endress Place, Greenwood, IN 46143, USA

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

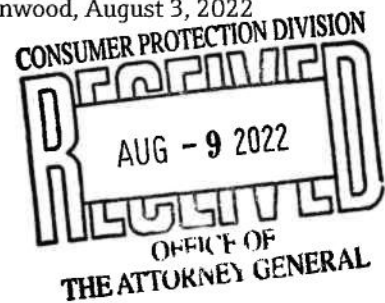
Contact

Krista S. Taggart
Deputy General Counsel
Phone: 317-619-9842
krista.taggart@endress.com

Greenwood, August 3, 2022

Re: Notice of Incident

Dear Sir/Madam:



I am writing to notify you of a security incident with respect to Endress+Hauser Optical Analysis, Inc. (formerly known as Kaiser Optical Solutions, Inc.) ("Endress+Hauser"), located in Ann Arbor, Michigan. Maryland residents may have been impacted by the security incident.

On July 6, 2022, Endress+Hauser was notified by its payroll provider, SinglePoint, that SinglePoint experienced a break-in at its office during which two SinglePoint laptops were stolen, and that the incident potentially resulted in a breach of personal data. According to the notice from SinglePoint, one laptop had been restored to factory settings and did not contain personal data. The second laptop was password-protected with a complex password; however, from a backup of the computer, it was determined that the second laptop contained W-2 print files for certain Endress+Hauser employees. SinglePoint promptly notified law enforcement of the break-in and law enforcement is currently investigating the incident. At this point, neither SinglePoint nor Endress+Hauser has any information to indicate that any personal data was accessed or misused. However, it is possible that personal data, including employee names and Social Security Numbers, may have been accessed by an unauthorized user; therefore, Endress+Hauser is notifying all potentially affected individuals of the incident. Endress+Hauser continues to work with SinglePoint to prevent a recurrence of this type of incident in the future.

Endress+Hauser will be mailing the attached notification letter to two Maryland residents in the next few days.

Please contact me at krista.taggart@endress.com or 317-619-9842 if you have any questions or request additional information.

Best Regards,



Krista S. Taggart



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-909-4423

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXX>>

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

August 3, 2022

Dear <<Name1>>:

SinglePoint is writing to inform that we recently identified and addressed an incident that may have involved some of your personal information. This notice explains the incident, the measures we have taken in response, and additional steps you may consider taking.

SinglePoint is an HR/Payroll Services company. On May 20, 2022, the SinglePoint office was broken into, and two laptops were stolen. One laptop had been restored to factory settings and did not contain any sensitive data. A second laptop was password protected with a complex password, however, from a backup, it was determined to have contained W2 print files for the employees of <<Variable Data 1>>. We do not currently have any information to indicate that the data was accessed or misused, however, it is possible the sensitive data, including names and Social Security numbers, could have been accessed by an unauthorized actor. Upon discovery of the incident, we immediately notified law enforcement, worked to determine what happened, the scope of data that was potentially accessed, and what steps can be taken to further safeguard our client data. We believe that the information contained on the laptop that could have been accessed by the unauthorized actor includes your name and Social Security number.

We are offering you one year of complimentary identity monitoring services through IDX. IDX identity protection services include: one year of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-909-4423 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. Please note the deadline to enroll is November 3, 2022. For more information on identity theft prevention, please see the pages following this letter.

We regret this incident occurred and apologize for any inconvenience. To help prevent something like this from happening again, we have implemented additional measures to enhance our existing security protocols.

If you have any questions, please call 1-833-909-4423 Monday through Friday from 9 am to 9 pm Eastern Time.

Sincerely,

SinglePoint

Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-909-4423 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft while your IDX identity protection membership is active, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 steps an individual can take to avoid identity theft as well as information 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. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

SinglePoint: 4006 N. Keystone Ave., Indianapolis, IN 46205.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

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). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, 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.

Endress+Hauser Optical Analysis, 371 Parkland Plaza, Ann Arbor, MI 48103, USA

[Click here to enter address.](#)

Contact

Jon McCullum
Vice President of Human Resources and
Finance
Phone: 317.670.7298
jon.mccullum@endress.com

Ann Arbor, August 3, 2022

Re: Potential Breach of Personal Information at Third-Party Payroll Provider

Dear Employee:

On behalf of Endress+Hauser, I am writing to notify you of a recent incident that may have impacted your personal data.

On July 7, 2022, Endress+Hauser received a notification letter from our payroll provider, SinglePoint, describing an incident potentially causing a breach of personal data. According to the SinglePoint notification, the SinglePoint office was broken into on May 20, 2022, and two laptops were stolen. One laptop had been restored to factory settings and did not contain any personal data. A second laptop was password protected with a complex password; however, from a backup, it was determined to have contained 2019 W2 print files for 104 Kaiser Optical employees.

At this point, SinglePoint and Endress+Hauser have no information to indicate that any of the personal data was accessed or misused. However, it is possible that personal data, including names and Social Security numbers, may have been accessible by an unauthorized actor. As soon as SinglePoint discovered that the laptops were stolen, SinglePoint immediately notified law enforcement. Law enforcement is investigating the break-in. As soon as Endress+Hauser was notified by SinglePoint, we immediately notified our internal Legal Department and we engaged outside legal counsel specializing in data privacy to provide guidance on the break-in incident and the protection of personal data.

Although at this time, we have no indication to believe that any of the personal data was actually accessed by an unauthorized actor, in full transparency, we wanted to alert you to the situation. You will be receiving a letter from SinglePoint containing further details on the incident and offering you the opportunity to enroll in complimentary credit monitoring membership through IDX. IDX identity protection services include: one year of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. We encourage you to enroll in this protection. Please note that you will not be enrolled automatically, you will have to sign-up for the IDX protection offered at no cost to you by SinglePoint as outlined in the instructions in their letter.

Please know that Endress+Hauser takes your data privacy and security very seriously. We are sorry that this incident occurred. We are currently working with SinglePoint to prevent a recurrence of this type of incident in the future. If you have any questions or concerns about this matter, please do not hesitate to reach out to me.

Best Regards,

Jon McCullum

DMS 23215678v2