

# ***Snap-on Incorporated***

P.O. Box 989728  
West Sacramento, CA 95798-9728

To Enroll, Please Call:  
(833) 676-2143  
Or Visit:  
<https://response.idx.us/snapon>  
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>  
<<ADDRESS1>>  
<<ADDRESS2>>  
<<CITY>>, <<STATE>> <<ZIP>>

April 7, 2022

## NOTIFICATION OF DATA BREACH

We write to inform you about a recent security incident, a part of which may have involved some of your personal data. In that regard, we want to make you aware of the actions the company is initiating, and of what steps you can take to raise your protection against inappropriate use of your data and identity theft.

We believe the incident involved associate and franchisee data including information such as: names, Social Security Numbers, dates of birth, and employee identification numbers. As is standard practice in this type of incident, we recommend you implement either a **fraud alert** or a **security freeze** on your credit. A fraud alert requires creditors to verify your identity before processing credit applications in your name, while a security freeze blocks access to your credit report altogether, except through your specific action.

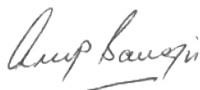
To assist you with these recommendations, we've arranged, at no cost to you, the option to enroll with **IDX**, an expert identity/credit protection service, for 24-month credit monitoring and fraud detection resources. IDX will provide for monitoring of all three credit bureaus, for fully managed fraud assistance, for identity theft reimbursement insurance, and for assistance in implementing further protections, including freezing and unfreezing credit.

We encourage you to contact IDX with any questions and to enroll in the provided protection services by calling (833) 676-2143 or going to <https://response.idx.us/snapon> using the enrollment code provided above. IDX representatives are available Monday through Friday from 8:00am to 8:00pm Central Time. The enrollment code above will be active for use until April 7, 2024.

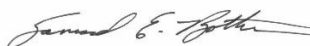
For more detail on the security incident, please see the "**Summary of Incident**" section of this letter. In particular, please review "What You Can Do" for further information on raising your protection.

We understand the importance you place on data security, and we take our responsibility to protect your information very seriously. We deeply regret any inconvenience or concern this matter may cause you.

Sincerely,



Anup Banerjee  
Senior Vice President –  
Human Resources and Chief Development Officer



Samuel E. Bottum  
Vice President and Chief Marketing Officer

## SUMMARY OF INCIDENT

**WHAT HAPPENED.** In early March, we detected unusual activity in some areas of our computer systems environment and quickly took down our network connections and launched a comprehensive analysis of the incident. During our review, we discovered that some personal data relating to our Snap-on people was taken by an unauthorized third party between March 1 and March 3, 2022.

**WHAT INFORMATION WAS INVOLVED.** We believe the incident involved associate and franchisee data including information such as: names, Social Security Numbers, dates of birth, and employee identification numbers.

**WHAT WE ARE DOING.** We've arranged, at no cost to you, for the option of enrolling in 24-month credit and fraud monitoring services. We've engaged IDX, a leading identity protection service, to provide you credit and CyberScan monitoring, which will provide for monitoring of all three credit bureaus, for fully managed fraud assistance, for a \$1,000,000 insurance reimbursement policy, and for assistance in implementing further protections, including freezing and unfreezing credit. Enrollment information can be found on the front of this letter.

This service will be available for the 24-month period following this notification. While you may activate the IDX service at any time during that period, should you enroll after the first 30 days, you will receive services for the remaining pro-rata portion of the program. Contact IDX at (833) 676-2143 to gain additional information about this event and to speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

Also, when we became aware of the incident, we promptly contained it, notified the Federal Bureau of Investigation, and engaged a leading external forensics firm to assist us in this matter. In addition to the defensive protocols deployed, we took the following measures to further harden our computer systems security:

- Quarantined global assets to contain the outbreak;
- Heightened monitoring technology on servers and workstations across all environments;
- Enacted a rigorous vetting process for bringing systems back online;
- Allowed network access for only those machines that were confirmed to be uncompromised;
- Strengthened authentication protocols.

**WHAT YOU CAN DO.** We recommend you enroll in the provided service. Please note that you will have to furnish personal data as part of that process. Credit monitoring, as well as assistance with fraud alerts and security freezes, are included in the IDX service. In addition, we recommend these ways to further protect yourself from data misuse and identity theft:

- *Avoid Phishing:* Please use caution when responding to third parties who request disclosure of your personal information via email, text or phone. This may include inquiries from third parties posing as company management, bank officials, information security experts, government agencies and other trusted sources, in an effort to trick you into divulging your personal information.
- *Be Cautious:* You should never provide personal information, such as usernames, passwords, government issued personal identification numbers (e.g., U.S. Social Security Numbers), account numbers or any other confidential personal information via email request or screen pop-ups. **Legitimate agencies/companies do not ask for this type of information in an email.**
- *Remain Vigilant:* Please remain vigilant for incidents of fraud. The IDX credit monitoring and fraud detection resources we're making available to you provide you with increased protection; nevertheless, in addition to regularly reviewing your IDX alerts (should you enroll), we recommend you review your account statements and your credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, and are enrolled in the identity protection program, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. Otherwise, be sure to report the activity immediately to your financial institutions.

If you file a request for help or report suspicious activity, you will be contacted by a member of the 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 as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop, and reverse the damage quickly.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s website, at [www.consumer.ftc.gov/identity-theft-online-security](http://www.consumer.ftc.gov/identity-theft-online-security), or call the FTC, at (877) IDTHEFT (438-4338) or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Whether or not you choose to enroll in the IDX service, you may implement these and other protection options using the information provided below:

You may periodically obtain credit reports from each nationwide credit reporting agency. Under the federal Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 <a href="http://www.Equifax.com/personal/credit-report-services">www.Equifax.com/personal/credit-report-services</a>	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 <a href="http://www.Experian.com/help">www.Experian.com/help</a>	TransUnion (888) 909-8872 Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19022 <a href="http://www.TransUnion.com/credit-help">www.TransUnion.com/credit-help</a>
--	--	--

You also have other rights under the FCRA. For other information about your rights under the FCRA, please visit: [http://files.consumerfinance.gov/f/201410\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf). You may also obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

***Fraud Alerts:*** You may place a **fraud alert** in your file by calling or visiting the website for 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. A fraud alert will help protect your credit information and can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. However, it also may delay your ability to obtain credit.

***Security Freezes:*** Additionally, you may contact the nationwide credit reporting agencies using the websites or phone numbers listed above to place a **security freeze** to restrict access to your credit report. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

**For those who enroll in the IDX service, you may call (833) 676-2143 for assistance with implementing these protections;** however, no one is allowed to place a fraud alert or security freeze on your credit report except you.

**FOR MORE INFORMATION.** Please call (833) 676-2143 or go to <https://response.idx.us/snapon> for assistance or for any additional questions you may have.

*IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT:* You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[http://consumer.ftc.gov/  
identity-theft-online-security](http://consumer.ftc.gov/identity-theft-online-security)

Office of the Attorney General  
441 4th Street, NW  
Suite 1100 South  
Washington, DC 20001  
(202) 727-3400  
<https://oag.dc.gov/>

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

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[http://consumer.ftc.gov/  
identity-theft-online-security](http://consumer.ftc.gov/identity-theft-online-security)

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

*IF YOU ARE A NEW YORK RESIDENT:* You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[http://consumer.ftc.gov/  
identity-theft-online-security](http://consumer.ftc.gov/identity-theft-online-security)

New York Attorney General  
Consumer Frauds &  
Protection Bureau  
120 Broadway, 3rd Floor  
New York, NY 10271  
(800) 771-7755  
[www.ag.ny.gov](http://www.ag.ny.gov)

New York Department of State  
Division of Consumer Protection  
99 Washington Avenue  
Suite 650  
Albany, New York 12231  
(800) 697-1220  
[www.dos.ny.gov](http://www.dos.ny.gov)

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

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[http://consumer.ftc.gov/  
identity-theft-online-security](http://consumer.ftc.gov/identity-theft-online-security)

North Carolina Department of Justice  
Attorney General Josh Stein  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
<http://www.ncdoj.com>

*IF YOU ARE A RHODE ISLAND RESIDENT:* You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General  
150 South Main Street  
Providence, RI 02903  
(401) 274-4400  
<http://www.riag.ri.gov/>