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

May 19, 2023

Re: Data Breach Report Submission

To Whom It May Concern:

On May 1, 2023 we discovered and resolved a cyber-incident on the following website https://www.omegawatches.com/en-us caused by a cyberattack on one of our service provider's former employees. Following investigations, we found **three (3)** New Hampshire residents potentially affected by a malicious script from April 25, 2023 through April 29, 2023 or from April 29, 2023 through May 1, 2023, respectively. The malicious script may have involved information entered while visiting our e-commerce website, including name and one or more of the following data elements:

In terms of steps taken: On May 1, 2023 we set up a task force to delete this malicious script and ensure all integrity of all of our websites. We have also changed passwords and credentials for our service providers and implemented additional technical safeguards. Enclosed please find a May 5, 2023 pre-notice and a May 19, 2023 notice.

Thank you,

Legal Department

Notice of Data Breach

[NAME]
[ADDRESS]
[ADDRESS]

[DATE]

Dear [FIRST NAME],

We recently became aware of a security incident affecting the information of certain customers. We are providing this notice to inform you of the incident and to call your attention to some steps you can take to help protect yourself. On behalf of The Swatch Group (U.S.) Inc., we sincerely regret any concern this may cause you.

WHAT HAPPENED. A malicious script was active from April 25,2023 until May 1, 2023 and detected on May 1, 2023 on the following website https://www.omegawatches.com/en-us caused by a cyberattack on one of our service provider's former employees that could have been used to scrape certain customer information identified below.

WHAT INFORMATION WAS INVOLVED. The incident may have involved information entered while visiting our e-commerce website, including your name and one or more of the following:

WHAT WE ARE DOING. We take the privacy of personal information held in our care extremely seriously. Therefore, we acted as promptly as possible and, upon discovery, removed the remaining active script from our e-commerce website. We also launched an investigation to identify the scope of any impact to our customers so that we could provide this notice. We have also changed internal passwords and credentials for our service providers, and implemented additional technical safeguards. We have informed the authorities as required.

WHAT YOU CAN DO. Please always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, we recommend that you change your password for any online account for which you use the same password that was used for MyOmega at the time of the incident.

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. ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the 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. In addition, under the Fair Credit Reporting Act, 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 . You may contact the nationwide credit reporting agencies at:

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

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. 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. You may place a fraud alert in your file by calling any of the 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. In addition, you can contact the nationwide credit reporting agencies regarding how you may place a security freeze to restrict access to your credit report.

FOR MORE INFORMATION. For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us directly at between 10:00 AM to 5:00 PM, Monday through Friday, or via email at .

Again, we sincerely regret any concern this event may cause you.

Sincerely,

RE: PRE NOTICE - CYBERSECURITY INCIDENT DETECTED ON E-COMMERCE WEBSITE DURING YOUR RECENT TRANSACTION ON OMEGAWATCHES.COM/EN-US

Dear Customer,

We, The Swatch Group (U.S.) Inc., operate the e-commerce website
which you have recently visited and on which you purchased OMEGA Product(s).

We are writing to inform you that we are currently investigating a cybersecurity incident which occurred between April 29, 2023 through May 1, 2023 and that may involve information that you have entered while visiting our e-commerce website, including your :

We have immediately, upon discovery, taken appropriate measures to correct the situation and initiated investigations with cybersecurity specialists. We are also informing the competent authorities.

In the meantime and as an added precaution you may consider taking the following measures:

- Be vigilant and contact your credit card companies if you notice suspicious activities;
- Contact your bank or credit card operator and request changing your card and blocking suspicious transactions;
- Be suspicious of communications from third parties claiming to have information about you;
- Change passwords.

We take the protection and proper use of your information very seriously and deeply regret that this incident occurred. We are committed to assisting you and if you have any question we remain at your disposal at

Sincerely,

Arnaud Michon

Brand President Omega

The Swatch Group (U.S.) Inc.

703 Waterford Way, Suite 450

Miami, Florida 33126

Hajra Patel

Chief Financial Officer

The Swatch Group (U.S.) Inc.

703 Waterford Way, Suite 450

Miami, Florida 33126