Dear Valued Customer,

We are writing to notify you of an incident involving your personal information.

Norton has intrusion detection systems in place to protect our customers and their data. These systems alerted us that an unauthorized third party likely has knowledge of the email and password you have been using with your Norton account (login.norton.com) and your Norton Password Manager. We recommend you change your passwords with us and elsewhere immediately.

What happened

On December 12, 2022, we detected an unusually large volume of failed logins to customer accounts. We quickly took steps to investigate, and on around December 22, 2022, we determined that, beginning around December 1, 2022, an unauthorized third party had used a list of usernames and passwords obtained from another source, such as the dark web, to attempt to log into Norton customer accounts. Our own systems were not compromised. However, we strongly believe that an unauthorized third party knows and has utilized your username and password for your account. This username and password combination may potentially also be known to others.

In accessing your account with your username and password, the unauthorized third party may have viewed your first name, last name, phone number, and mailing address. Our records indicate that you utilize our Norton Password Manager feature and, we cannot rule out that the unauthorized third party also obtained details stored there especially if your Password Manager key is identical or very similar to your Norton account password. If your data has been accessed, the unauthorized third party could make this data available to other unauthorized parties or use the password and email combination to try to access your other online accounts.

Steps we have taken

To protect you best, early in our investigation, we quickly reset your Norton password in order to prevent additional attempts to access your account by the unauthorized third party. In addition, we took numerous measures to counter the efforts of these unauthorized third parties and to impede their efforts to validate credentials and access accounts. We care deeply about your Cyber Safety and work to provide the best security for your data, such as offering two-factor authentication which we strongly encourage you to use. We are making a credit monitoring service available to you. If you would like additional information about this incident, or information on credit monitoring please contact our customer service (contact details below). This notification was not delayed as a result of a law enforcement investigation.

What you should do

We recommend urgently changing your password, not only with Norton, but also on all other sites where you may have used the same password. All passwords stored in Norton Password Manager should immediately be changed.

Practicing password hygiene — such as changing passwords on a regular basis, not using the same password more than once, and using unique and complex passwords— is highly recommended, and makes it less likely an unauthorized third party could gain access to accounts across services that use the same password. We also recommend implementing two-factor authentication for an added layer of security.

For more information

If you would like additional information about this incident, or information about credit monitoring, please contact us at norton_escalation@gendigital.com or 1-800-607-8094.

- Your Norton Team

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements**

As a precautionary measure, we recommend that you review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, or the Federal Trade Commission. In some states, you may also obtain a police report regarding this incident.

- **Credit Report Monitoring**

You may obtain a free copy of your credit report from each of the 3 major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies shown below.

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC's Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357), or for more information about identity theft, please visit http://www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338).

For residents of the District of Columbia, the Attorney General for the District of Columbia can be contacted at: 400 6th Street, NW, Washington DC 20001; (202) 727-3400; oag@dc.gov; https://oag.dc.gov/.

- **Fraud Alert**

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- **Security Freeze**

Pursuant to federal law, you have the right to put a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.