
Notice of Data Security Incident Affecting Maryland Residents

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

VIA E-MAIL: idtheft@oag.state.md.us

November 8, 2023

Re: Notice of Data Security Incident Affecting Maryland Residents

Dear Maryland Security Breach Office representative:

I am writing to notify you of a data security incident involving five Maryland residents. I am an attorney for LEGO BrickLink, Inc. (“BrickLink”), an online marketplace service exclusively for LEGO® building toy products, through which member buyers and sellers conduct transactions. LEGO BrickLink is a wholly owned subsidiary of LEGO Systems, Inc. of Enfield, Connecticut. BrickLink’s main business office is at 16815 Von Karman Avenue, Suite 100, Irvine, CA 92606.

On Friday, November 3, 2023, an unknown individual (the “bad actor”) posted a notice on the BrickLink member Discussion Forum, claiming to have breached the security of the website BrickLink.com, and threatening to delete data and disrupt operations unless we paid a ransom of €50,000 (approximately \$53,600 USD). BrickLink staff immediately took the site offline for investigation, isolating it from any further outside intrusion. Upon investigation, we determined that

the bad actor had obtained login information for several BrickLink accounts through unknown means external to the BrickLink operation. We have reason to believe that the bad actor has hijacked a few seller accounts, and may have received payments for orders from unsuspecting buyers, and then kept the funds without shipping any products. We paid no ransom, and we have reported the incident to the Internet Crime Complaint Center at IC3.gov.

BrickLink remains offline as of this writing, but we intend to restore access to it later today. When we do so, all members will be logged out, and will be required to reset their passwords before regaining access to their BrickLink accounts. For those accounts known to have been directly impacted by this incident, we will require a two-factor authentication process prior to restoring account access.

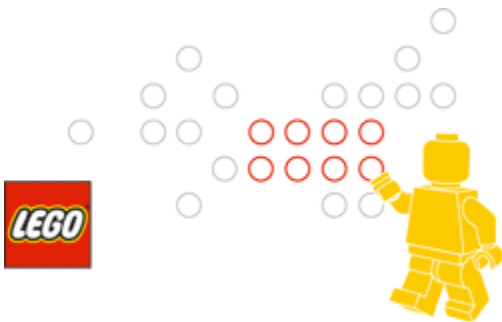
Our investigation determined that BrickLink accounts belonging to five Maryland residents were among those that had been compromised. Having obtained the Maryland residents' passwords for their BrickLink accounts, the bad actor would have had access to such personal information as first and last names, residence addresses, email addresses, and phone numbers. The bad actor would not have been able to obtain such highly sensitive information as the members' social security numbers or bank, credit card, or other payment or financial information.

In response to the breach, we have instituted a number of enhanced security measures, including the password reset requirement mentioned above. We will provide written notice of this incident to the affected individuals using the form notification template attached hereto. We will also be posting an explanation for the extended outage of the BrickLink service along with information on how to avoid being victimized online, and encouraging members to contact us with any questions. Although it is still early in our investigation and response, we are considering requiring two-factor authentication for site logins across the board.

Please let me know if you have any questions about this data security incident or LEGO BrickLink's response.

With kind regards.

Robert Nielson
Associate Corporate Counsel
LEGO Systems, Inc. and LEGO BrickLink, Inc.



Robert Nielson
Associate Corporate Counsel
Americas Markets

Direct +18607636746

Mobile +18602994670

E-mail Robert.Nielson@lego.com

LEGO Systems, inc.

100 Print Shop Road

Enfield, CT 06082

United States

www.LEGO.com

LEGO and the LEGO logo are trademarks of the LEGO Group. ©2023 The LEGO Group.

This email message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system.

Email subject: Update from BrickLink ACTION required.

Dear [member name]:

We're writing to let you know that BrickLink is back up and running and that we look forward to seeing you back on the site!

We temporarily closed the site on November 3rd due to some unusual activity. After thorough investigation we found that a relatively small number of accounts potentially may have been accessed by unauthorized individuals using data obtained outside the BrickLink platform.

Unfortunately, your account might have been impacted.

As a precaution we've temporarily locked your account. To re-open it, please go to the BrickLink site and start the process of reopening your account by following the prompts during login.

If you have a seller account, please check your inventory and if you believe it has changed or been deleted, please email customerservice@bricklink.com. We will do what we can to help restore your inventory.

Once you've re-gained access to your account please check your inventory if you have a seller account and reach out to customerservice@bricklink.com if you believe the inventory has been changed or deleted, we will do what we can to assist you with restoring your inventory to a specific date.

You can get help on this and other topics in the related help page or read more in the BrickLink Forum after re-opening your account.

Thank you again for your support and patience. We are grateful to have such awesome members!

Thanks!

Your BrickLink team

What information may have been accessed?

Account information:

Name

Email address

Country

Billing & delivery addresses

Order history

Phone number

We do not store complete credit card details on BrickLink, so these cannot be accessed.

If you have any questions or concerns, please contact LEGO® BrickLink Inc. at customerservice@bricklink.com

What is BrickLink doing in response?

We've already taken steps to further strengthen our security; and we continue to investigate and take steps to tighten how we monitor and respond to unusual activity.

We've stepped up our account security and monitoring of unusual activity, informed people whose accounts or stores may have been impacted, and reminded members of ways they can make their accounts safer and more secure by practicing good data security. Install and run security software on their devices and create strong, unique passwords only used on the BrickLink site.