Dear Armor Gamers,

Armor Games is taking steps to notify its users of a recent event that affects the security of its users' data. While much of the data affected is public profile information, it includes usernames, emails, hashed passwords and the salt (allowing the hashed passwords to be reversed). We care deeply about our users' security and are taking numerous steps to prevent this from happening again and to protect against the misuse of information.

What happened? On January 29th, 2019, Tuik Security Group privately contacted us to let us know about a potential breach of our users' data. We immediately began an investigation which included an ongoing audit of our hosting provider, web servers, and database systems. We can now confirm this breach is real and occurred around January 1st, 2019. This appears to be part of a larger breach affecting 16 companies (see this news article for more information). We are one of the smaller companies affected, apparently holding less than 2% of the total accounts affected between the 16 companies. At this time, we have no evidence that any Armor Games' users' data was actually misused and we are taking steps to prevent potential misuse.

What information was involved? The database affected primarily stores all our website users' public profiles (information that is already public), login data (usernames, email addresses, IP addresses, and hashed passwords), birthdays of our admin accounts, and information about our password protection processes (including the password salt). We do not have (and thus, we believe this incident does not involve) first or last names, credit card data, addresses, or phone numbers.

Based on public reporting, the other companies affected by this breach similarly included account information, hashed passwords, and the salt to reveal those passwords. In addition, some of the accounts held by the other companies appear to include names, social media authentication tokens, security questions and answers, interests, profile information, birthdays, and location data.

What we are doing. While we investigate, we will require our users to update their passwords. We are making changes on our side to harden our security and fixing any weaknesses found by our audit, including updating our password protection methods. We are also adding measures to protect our users from misuse of this information on our own site. We have begun notifying authorities and will cooperate with law enforcement if requested and we may work with the other companies affected. We already have a policy of keeping as little data as possible and we will continue to look for new ways to minimize our data collection.

What you can do. We recommend taking this opportunity to update your passwords on all websites. Use unique, creative passwords and avoid reusing passwords across websites (password managers can help make this easy). Those who reuse passwords should change their passwords on other services, especially other gaming platforms. In addition, we recommend learning whether any of the other companies affected by this breach include your data, following their instructions for securing your account information. As always, you have the right to request to access or delete your data from us at any time.

Learn about other affected companies. Based on this news article, we are one of 16 separate companies affected. If you have accounts with any of the companies in this breach, please look for a separate breach notification from them or reach out to them for instructions.

Report suspected fraud. We have no evidence of, and it appears unlikely that, the information could be used to commit identity or financial fraud. However, if you experience identity fraud (from us, the other companies involved, or in general):

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

You also have the right to place fraud alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting: 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348
www.alerts.equifax.com

Experian Fraud Reporting: 1-888-397-3742 P.O. Box 9554 Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting: 1-800-680-7289 P.O. Box 2000 Chester, PA 19022
www.transunion.com

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. 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. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze. W9894 v.04 02.06.2019 6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies.

Report Misuse of Data. The Federal Trade Commission encourages those who discover that the leaked information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.

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

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

For More Information. If you have any questions or concerns, please reach out to us at support@armorgames.com, our preferred method of contact. You can alternatively mail us at 16808 Armstrong Ave. Suite #205, Irvine CA 92606. Maryland users can call us at (949) 529-1718.

ArmorGames sincerely apologizes for the inconvenience and concern this incident may cause, and remains committed to safeguarding the personal information in its care. We will notify you of any significant developments. We continue our work to be the best place to play free web games online.