



March 1, 2016

[Employee]  
[Address]  
[Address]

**Notice of Data Breach**  
**Payroll Information Disclosed via 3rd Party Scam**

Dear [Name]:

**What Happened**

As you know from the email we sent you last Friday (February 26, 2016), earlier that day Snapchat's payroll department was targeted by an isolated email phishing scam in which a scammer impersonated our Chief Executive Officer and requested that employee information be sent via email. It did not affect our users or our service whatsoever.

The result of this scam was that payroll information about some current and former employees was improperly disclosed externally. None of our internal systems were breached, and no user information was accessed. We are obviously very sorry that this happened and we are doing everything we can to work with our team to prevent any similar incident from occurring in the future.

We are continuing to investigate the incident. In the meantime, we are offering to all impacted current and former employees free identity-theft monitoring and insurance for two years. You'll find instructions on how to sign up for both under the "What You Can Do" heading in this letter.

**What Information Was Involved**

The scammer has obtained the following information about you: your name, Snapchat employee ID, Social Security number, state of residence and work, and 2015 wages earned, including stock-option gains, if any. The scammer also obtained other information: costs of company-paid benefits for life and health insurance; relocation reimbursements; employee contributions to retirement, dependent care, and healthcare plans; additional required payments; and taxes withheld from your earnings.

## **What We Are Doing**

To protect your information, we have responded promptly and aggressively. Within four hours of this incident, we confirmed that the phishing attack was an isolated incident and reported it to the Federal Bureau of Investigation.

We are offering two years of free identity-theft insurance and credit monitoring through ID Experts. ID Experts' MyIDCare program will monitor all three credit-monitoring bureaus, provide up to \$1 million in reimbursement for fraudulent charges, and provide identity-restoration services should you suffer identify theft or fraud. It also includes monitoring of your personal information online and access to educational information on the member website.

## **What You Can Do**

You can enroll by visiting the ID Experts website at <https://www.idexpertscorp.com/enrollment> [REDACTED]. You can also contact ID Experts with questions or enroll by phone at 866-328-1984. ID Experts is available weekdays 6 am-6 pm Pacific Time. Please note the deadline to enroll is May 1, 2016.

We strongly encourage you to enroll in this free service. If, however, you choose not to, we encourage you to monitor your credit reports and other financial records for fraudulent transactions. You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling toll-free 877-322-8228. Review the reports carefully. If you find anything you do not understand or that is incorrect, contact the appropriate credit reporting agency. If you suspect fraudulent activity, you can contact local law enforcement, your state's attorney general, and the Federal Trade Commission.

You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account, but might also delay any requests you make for new accounts. Inquire with the credit-reporting agencies for their specific procedures regarding security freezes.

- Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (391-3742); [www.experian.com](http://www.experian.com); Fraud Victim Assistance Division, P.O. Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

## For More Information

The Federal Trade Commission also provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen.

The Federal Trade Commission  
Identity Theft Clearinghouse  
600 Pennsylvania Avenue NW  
Washington, D.C. 20580  
[www.consumer.ftc.gov](http://www.consumer.ftc.gov)  
1-877-ID-THEFT (877-438-4338)

You may also contact us, of course, with any questions. Current Snapchat employees, please email [REDACTED]@[snapchat.com](mailto: [REDACTED]@snapchat.com). Former Snapchat employees, please email [REDACTED]@[snapchat.com](mailto: [REDACTED]@snapchat.com).

We are very sorry that many of our employees and former employees have been affected by this unfortunate incident. We stand ready to answer your questions and to help you find solutions to any problems that arise.

Sincerely,



Chris Handman  
General Counsel