August 8, 2019

Notice of Data Breach

Dear [NAME]

I wanted to reach out personally to follow up on the email you received from us on August 3, 2019 and to provide you with additional information about the data security incident we recently discovered.

First, let me say how much we regret that you are dealing with this issue at all. We take the trust you place in us very seriously, and this is not the kind of experience we want for our community.

While we have worked to do everything we could to best protect our customers, when we first communicated with our customers we did not have much information, which unfortunately is a frustrating reality of data incidents. I hope the facts below will provide better clarity into the timeline and our actions, but regardless, I do want to deeply apologize for any confusion. When we were first alerted to suspicious activity, we focused on identifying and taking proactive measures to protect the StockX community, which included a system-wide update and password reset. We also engaged third-party experts to investigate the suspicious activity to determine what happened and how serious it was. I am proud of our team for focusing on protecting the customer first, and I apologize for any ambiguity that resulted from our initial communication.

That is also why, even though we are still continuing to conduct a full investigation into the nature and scope of what happened, I want to send this notification now. I hope this will provide you with additional facts about the incident, steps we took in response to protect you, and measures we are taking to remediate any potential effects of this suspicious activity. I also want to assure you that we have contacted, and are working with, law enforcement to hold these illicit actors responsible, and have notified, or are notifying, appropriate regulators of the incident.

Please know how important you are to this community, and that your privacy and security are a top priority for us. Below you will find additional information about the incident and guidance on steps you can take to further protect yourself, as well as an offer from us for 12 months of free fraud detection and identity theft protection for added peace of mind. We stand ready to answer questions you may have.

What Happened?

On July 26, 2019, StockX was alerted to suspicious activity potentially involving customer data. We immediately launched a forensic investigation and engaged experienced third-party experts to assist. During this first week, while our forensic investigation into the suspicious activity was underway, we took proactive and precautionary measures to protect our customers. As described in greater detail in the "what are we doing" section below, we deployed a system-wide update, implemented a full password reset of all customer passwords for all StockX accounts, and on the morning of August 1, 2019 sent customers an email alerting them to the systems update and password reset.

As our investigation continued, forensic evidence revealed that an unknown third party had been able to gain unauthorized access to certain customer data from our cloud environment on or around May 14, 2019. We worked swiftly to issue an email update of the matter to our customers and are now making this notification to further apprise you of additional facts from our investigation.

As part of our efforts to catch the perpetrator, we have contacted law enforcement and have been working with them in their investigation of the incident. Our investigation into the nature, extent, and scope of the incident remains ongoing, and we will update you with additional information as necessary.

What Information Was Involved?

From our investigation to date, the information affected may include your name, email address, address, username, hashed password, and purchase history.

As indicated in our prior communications, there is no evidence to date to suggest that any of your financial or payment information has been affected. That is because StockX does not store full payment card or financial data of its customers on its network servers or platform. Instead, any StockX payment card data is processed, stored, and hosted by a third-party payment processor, and not StockX. Based on our investigation to date, we have no evidence to suggest that our third-party payment processing partners or our third-party platform has been affected by this incident, nor do we have any evidence to suggest that any of the customer financial or payment information stored by that third-party has been affected.

What Are We Doing?

As previously described, upon first learning of the suspicious activity, we immediately launched an internal forensic investigation into the reported activity. On the same day, we engaged third-party data incident and forensic experts to assist with the investigation.

While we were conducting our forensic investigation into the suspicious activity, out of an abundance of caution, we took proactive steps to implement infrastructure changes to mitigate and address any potential effects of the suspicious activity. These infrastructure changes included:

1. a system-wide security update;
2. a full password reset of all customer passwords, with an email to customers alerting them about resetting their passwords;
3. high-frequency credential rotation on all servers and devices; and
4. a lockdown of our cloud computing perimeter.

We also contacted law enforcement and have been working with them in their efforts to catch the perpetrator. While law enforcement was involved, this notice was not delayed at the request of a law enforcement agency or as a result of a law enforcement investigation.

Once the investigation revealed evidence to suggest customer data may have been accessed by an unknown third party, we sent you an email on August 3, 2019 to make you aware of the incident and provide you with the information we had at the time and guidance on the steps we were taking—and you could take—to protect your data.

As our investigation has continued, we are now providing you this notice to give you further information about the facts and how you can protect yourself and your personal information. Additionally, we have notified, or are notifying as necessary, any appropriate regulators in the United States, the European Union, and other impacted foreign jurisdictions.

We are offering you free fraud detection and identity theft protection. As a precautionary measure, we are offering you **12 months** of **free** fraud detection and identity theft protection through ID Experts®, the data breach and recovery services expert, to provide you with their MyIDCare™ product. MyIDCare services include: CyberScan

monitoring, fully managed id theft recovery services, a $1,000,000 insurance reimbursement policy, and 12 months of free credit monitoring. With this protection, MyIDCare will help you resolve issues if your identity is compromised. We encourage you to contact ID Experts with any questions and to enroll in the free MyIDCare services by calling **(833) 300-6935** (if you are calling from the United States) or **+1-971-317-8411** (if you are calling from outside of the United States) or by going to **https://ide.myidcare.com/stockx.** Please note the deadline to enroll is **November 8, 2019.**

What You Can Do

Again, we take very seriously the security and privacy of your information, and want to make sure you have the information you need so that you can take steps to help protect your personal data. Because of the proactive mitigation and response steps we have taken, and the nature of the incident based on the forensic evidence we have today, we believe that the consequences of the incident and risk to individuals is low. Nevertheless, and even though the passwords affected were hashed, we recommend that if you use your StockX password for other accounts, you change those passwords as well.

As always, we encourage our customers to remain vigilant by reviewing their account statements and credit reports closely. So that you can take proactive steps to help protect your personal information, at the end of this letter we have provided you with additional information regarding steps you can take to further protect yourself. We encourage you to review that additional information.

For More Information

Your trust is at the center of our business, and we want to make sure you get answers to any questions you may have. So, we have set up a dedicated call center to answer questions regarding this incident. If you have any questions about the incident or this notice please call **(833) 300-6935** (if you are calling from the United States) **or +1-971-317-8411** (if you are calling from outside of the United States).

We deeply regret the inconvenience or concern that this incident might cause you.

Sincerely,

Scott Cutler
Chief Executive Officer
1046 Woodward Avenue
Detroit, Michigan 48226

GDPR-Related Contact Information
Olivier Van Calster
Data Protection Officer
StockXUK Ltd
5 New Street Square, London, United Kingdom, EC4A 3TW
dpo@stockx.com
+1-971-317-8411

Additional Steps You Can Take to Protect Your Personal Information

Report Suspicious Activity or Suspected Identity Theft. If you detect any unauthorized or suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. If you suspect any identity theft has occurred, you can contact your local law enforcement by filing a police report or the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338), by writing to the FTC at 600 Pennsylvania Avenue, NW Washington DC 20580, or online at www.ftc.gov. You can also contact your state Attorney General.

Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, NC 27699.

Rhode Island residents may wish to review information provided by the Rhode Island Attorney General at http://www.riag.ri.gov, by calling 401-274-4400, or by writing to 150 South Main Street, Providence, RI 02903.

Credit Reports: Under U.S. federal law, you are entitled to one free copy of your credit report every 12 months. You can request a free credit report once a year at www.annualcreditreport.com, by calling (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.

You may also contact the three U.S. credit reporting agencies to request a credit report:

- TransUnion LLC, P.O. Box 1000, Chester, PA 19016; (800) 888-4213; https://www.transunion.com/#
- Experian, P.O. Box 4500, Allen, TX 75013; (888) 397-3742; https://www.experian.com/consumer-products/free-credit-report.html
- Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30348-0241; (888) 349-5191; https://www.equifax.com/personal/credit-report-services/

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud alerts: As a precautionary step, to protect yourself from possible identity theft you can place a fraud alert on your bank accounts and credit file. A fraud alert tells creditors to follow certain procedures before opening a new account in your name or changing your existing account. You may call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. All three credit reports will be sent to you, free of charge, for your review.

- TransUnion Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19016; (800) 680-7289; https://www.transunion.com/fraud-victim-resource/place-fraud-alert
- Experian, P.O. Box 4500, Allen, TX 75013; (888) 397-3742; https://www.experian.com/fraud/center.html
- Equifax, P.O. Box 105069, Atlanta, GA 30348-5069; (888) 836-6351 or (800) 525-6285; https://www.equifax.com/personal/credit-report-services/

Credit/security freeze: In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. 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 apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. To put a security freeze on your credit file contact the consumer reporting agencies listed below.

- TransUnion, P.O. Box 160, Woodlyn, PA 19094; (888) 909-8872; https://www.transunion.com/credit-freeze/
- Experian, P.O. Box 4500, Allen, TX 75013; (888) 397-3742; https://www.experian.com/freeze/center.html
- Equifax, P.O. Box 105788, Atlanta, GA 30348-5788; (888) 298-0045 or (800) 349-9960; https://www.equifax.com/personal/credit-report-services/