



ASOS US SALES LLC

97N 10th Street
Brooklyn NY 11249
United States

August 21, 2026

Re: Notice of data breach from ASOS US Sales LLC

Dear Washington Attorney General's Office,

I am writing behalf of ASOS US Sales LLC to inform you of a recent data security incident that affected some ASOS customers in your state.

Name of business: ASOS US Sales LLC
300 Creek View Road, Suite 209
Newark, Delaware, 19711, USA

Date(s) of incident: July 28, 2026–July 29, 2026

Date of discovery: July 28, 2026

Date of individual notice: By August 24, 2026

Was notification delayed because of law enforcement investigation? No

Type of personal information involved: Name, delivery or billing address, telephone number, redacted payment card details (cardholder name, last four digits of payment card, and expiration date), details of associated social media accounts (but *not* login credentials), and date of birth.

Brief description of the incident: On Tuesday, July 28, 2026, ASOS detected an increased level of unusual traffic on our website, www.asos.com. We immediately began an investigation. On Wednesday, July 29, 2026, we confirmed that someone tried to use credentials acquired from a source outside ASOS to access ASOS customer accounts. Fortunately, they were largely unsuccessful. Of the affected accounts, most did not experience anything beyond an unauthorized login. Only 104 US accounts (including 2 Washington accounts) experienced attempts to amend customer data. Unauthorized orders were placed on only 55 accounts worldwide (including 0 Washington accounts), which were detected and canceled automatically or manually.

Number of affected customers: 138,828

ASOS US Sales LLC
Registered office: 300 Creek View Road, Suite 209, Newark DE 19711 No. 5476654
State ID: B20260039235 (California) 17103489 (Georgia) 4528246 (New York)





Number of affected state residents: 117,802 (including 1,929 Washington residents)

Type of entity: Clothing retailer

Is the organization a small business? No

Type of breach: Credential-stuffing attack

Was the personal information accessed encrypted? Yes, encrypted in transit and at rest.

Severity of incident: The incident is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence. The incident did not affect critical infrastructure, emergency operations, or emergency communications.

Action taken to remediate the incident: Whilst ASOS employs market leading anti-bot tools to prevent attacks of this sort, it appears that those controls had been circumnavigated by a sophisticated attack methodology employing residential proxy botnet coupled with an extended header to bypass our preventative and detective controls. The attack was quickly identified by our monitoring Security Operations Centre and we took swift action to block the problematic user-agent and to prevent the attack propagating to further accounts whilst our anti-bot tool provider investigated the vulnerability exploited by the attacker.

Following discovery of the attack, ASOS took prompt action to block all of the affected customer accounts and impose a mandatory password reset across all of these accounts. This was completed during the course of Wednesday, July 29. ASOS emailed the affected customers on Thursday, July 30 to notify them that they would need to reset the password on their account in order to access the account again. In a small number of cases, the affected accounts were blocked permanently and the customers were asked to create new accounts.

The activity was being monitored by multiple teams while Cyber Security were actively investigating the CDN behavior and creating rules to mitigate the attack. As explained above, we implemented technical steps which prevent the attack propagating further. Since implementing this rule, we have not seen any further attack attempts. Our third party anti-bot tooling provider has implemented new rules to prevent such attacks from occurring in the future.

In addition, we have implemented new controls on our website to improve our customers' password hygiene (for example, by preventing the reuse of old passwords).

ASOS US Sales LLC

Registered office: 300 Creek View Road, Suite 209, Newark DE 19711 No. 5476654
State ID: B20260039235 (California) 17103489 (Georgia) 4528246 (New York)





Was substitute notice given? No

Was media notice given? No

Was law enforcement notified? No

Was a police report filed? No

Company contact. Anna Sewell, Head of Data Privacy and Compliance, ASOS,
anna.sewell@asos.com.

Very truly yours,

Anna Sewell

ASOS US Sales LLC

Registered office: 300 Creek View Road, Suite 209, Newark DE 19711 No. 5476654
State ID: B20260039235 (California) 17103489 (Georgia) 4528246 (New York)



ASOS US SALES LLC
97N 10th Street
Brooklyn NY 11249
United States

August 21, 2026

[NAME]
ADDRESS
EMAIL]

Re: **Important Notice ASOS US Sales LLC**

Dear [NAME],

I'm writing on behalf of ASOS US Sales LLC and our affiliate, ASOS.com Limited, to let you know that information associated with your ASOS account may have been accessed by an unauthorised third party.

On Tuesday, July 28, 2026, we detected unusual activity involving your ASOS account and immediately began an investigation. On Wednesday, July 29, 2026, we confirmed that an unauthorized third party may have gained access to your account using login credentials obtained from a source outside ASOS. We have since secured your account and are contacting you because information associated with your account may have been affected.

On July 29, our security operations team blocked access to your account and imposed a mandatory password reset. We emailed you on Thursday, July 30, to notify you that you would need to reset your passwords. Where we saw evidence of suspicious transactions, either the transactions were blocked automatically, or our fraud personnel canceled them manually. We have seen no additional unauthorized activity since we took these steps.

Erring on the side of caution, we want to let you know there may have been unauthorized access to information associated with your account, possibly including your name; email address; delivery or billing address, telephone number; the last four digits of payment card and expiration date), and details of associated social media accounts (but *not* login credentials) or date of birth if you saved that information in your account. While we believe this issue has been resolved, we recommend you monitor your payment account activity and statements for anything unusual.

We also want to remind you that the three major credit reporting bureaus, Equifax, Experian, and TransUnion provide free services that may assist you. Under federal law, you are entitled to one free credit report annually from each of them. A free credit report lets you check whether:

- Someone has opened accounts or taken loans in your name;
- There are unfamiliar credit cards, addresses, or searches on your file;
- Your personal details are being used fraudulently; and/or
- Your credit score or history has changed unexpectedly.

To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

You may also contact the credit bureaus to place a fraud alert or credit freeze on your credit file at no charge under federal law. A fraud alert is a 1-year (or longer) alert on your credit file that requires businesses to take added steps to verify your identity before extending new credit. A credit freeze prevents a credit bureau from releasing information about your credit history without your consent. You should know, however, that using a credit freeze to take control over who gets access to personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of a later request or application for a new loan, credit, mortgage, or any other credit account.

Please know that ASOS takes your privacy seriously and regrets any inconvenience caused by this incident. If you have any questions about this incident or we can help you in any way, please reach out to us at:

ASOS US Sales LLC
97N 10th Street, Brooklyn, NY 11249, United States
<https://www.asos.com/us/customer-care/get-in-touch/>

Additional information

Federal Trade Commission

The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint. For more information:

1-877-ID-THEFT / 1-877-438-4338

www.identitytheft.gov

TTY: 1-866-653-4261

600 Pennsylvania Avenue NW, Washington, D.C. 20580

For information on your rights under the Fair Credit Reporting Act:

www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Consumer Response Center, Room 130-A

Federal Trade Commission 600 Pennsylvania Ave. N.W.

Washington, D.C. 20580

Credit reporting agencies

Equifax 1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/>

Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069;

Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788.

Experian 1-888-397-3742

<https://www.experian.com/help/>

Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013

Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013.

TransUnion 1-800-916-8800

<https://www.transunion.com/credit-help>

TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

State-specific information

Colorado. You may obtain one or more additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

District of Columbia. You can obtain additional information about the steps you can take to avoid identity theft from the DC Office of the Attorney General at <https://oag.dc.gov/consumer-protection/consumer-alert-identitytheft>.

District of Columbia Attorney General
400 6th Street, NW
Washington, D.C. 20001
202-727-3400
<https://oag.dc.gov>

Georgia. As noted above, you may obtain a copy your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Iowa. Report any suspected identity theft to local law enforcement, your Attorney General, and the Federal Trade Commission.

Iowa Attorney General
Director of Consumer Protection Division
1305 E. Walnut Street; Des Moines, IA 50319
1-515-281-5926
www.iowattorneygeneral.gov

Maryland. You may obtain information from the Maryland Office of the Attorney General about steps to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
<https://oag.maryland.gov/i-needto/Pages/identity-theft-information.aspx>.

New Jersey. As noted above, you may obtain a copy your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

New Mexico. Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right

to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York. In addition to placing a security freeze on your credit report, as described above, you may report any incidents of suspected identity theft to the Federal Trade Commission, New York Attorney General, or local law enforcement.

You may obtain information about security breach response and identity theft prevention and protection from:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue, Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina. You may obtain information about preventing identity theft from the North Carolina Attorney General's Office.

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226 or 1-919-716-6000
www.ncdoj.gov

Oregon. You are advised to report any suspected identity theft to local law enforcement, your Attorney General, and the Federal Trade Commission.

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392
www.doj.state.or.us

Rhode Island. You may obtain a police report regarding this incident.

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

As of the date of this mailing, the approximate number of Rhode Island residents receiving this mailing is 334.

Vermont. Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/>.

Vermont residents who do not have internet access but would like to learn more about how to place a security freeze on your credit report may contact the Vermont Attorney General's Office at 800-649-2424 (toll free in Vermont only).

Wyoming. This notice was not delayed by law enforcement.