
SEARS HOLDINGS

Jeremy R. Holbrook
Deputy General Counsel
Law Department
Sears Holdings Management Corporation
3333 Beverly Road, B6-234B
Hoffman Estates, IL 60179
Direct Dial: 847.286.6356
Fax: 847.286.3439
Email : Jeremy.Holbrook@searshc.com

May 3, 2018

VIA UPS NEXT DAY AIR AND E-MAIL: consumer@ag.iowa.gov

Consumer Protection Division
Security Breach Notification
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

Dear Attorney General Miller:

On behalf of Sears Holdings (“Sears”), I am writing to inform you of a data security incident, in connection with which Sears is notifying 713 Iowa individuals of a potential compromise of their payment card information.

In mid-March, one of our vendors providing online support services on our websites at Sears.com and Kmart.com (collectively, the “Sites”) notified Sears that it had experienced a security incident in which an unauthorized individual was able to incorporate a malicious script into our vendor’s code which was used to provide certain services on our websites.

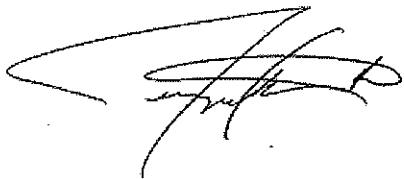
As soon as Sears learned of this incident, we conducted a thorough investigation of the incident. On March 26, 2018, Sears discovered that the malicious script could enable this unauthorized individual to collect certain customers’ names, addresses, and payment card information. The investigation concluded that the incident affected customers on the Sites who placed or attempted to place an online order between September 27, 2017 and October 12, 2017 and entered their payment card information manually on the checkout screen. Sears has notified the credit card companies of this incident, and our vendor has assured us that it has removed the script from its code and secured its systems. There is no evidence that our stores were compromised or that any internal Sears systems were accessed by those responsible.

We have sent a notification letter to each affected individual for whom Sears had sufficient contact information. A generic sample copy of this notification letter is enclosed. Sears does not have sufficient information to identify any additional Iowa customers who attempted to

place an order but the payment card was declined, and therefore is providing substitute notice as set forth in state law.

If you have any questions, please contact me at 847.286.6356 or Jeremy.Holbrook@searshc.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeremy R. Holbrook". The signature is stylized with a large, sweeping initial "J" and "H".

Jeremy R. Holbrook
Deputy General Counsel

Enclosure



3333 Beverly Rd
Hoffman Estates, IL 60179

April 25, 2018

D7052-L02-0123456 0001 00000001 *****MIXED AADC 159
SAMPLE A SAMPLE - GENERAL WITH APPENDIX



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Important Payment Card Security Notification.
Please read this entire letter.

Dear Sample A Sample,

Sears Holdings (“Sears”) was recently notified, by a vendor providing online support services on our websites at Sears.com and Kmart.com, that the vendor had experienced a security incident in which an unauthorized individual incorporated a malicious script into our vendor’s code which was used to provide certain services on our websites. The malicious script collected names, addresses, and payment card information. You are receiving this letter because our records show that information about your Card Type ending in ##### may have been affected by this incident.

As soon as our vendor informed us of this incident in mid-March, Sears notified the payment card companies to help prevent potential fraud, and conducted a thorough investigation of the incident. The investigation concluded that the incident affected some customers on Sears.com and Kmart.com who completed an online order between September 27, 2017 and October 12, 2017 and entered their payment card information manually on the checkout screen. Our vendor has assured us that it has taken steps to secure its systems and prevent this type of incident from occurring again in the future. There is no evidence that our stores were compromised or that any internal Sears systems were accessed by those responsible.

We are cooperating with law enforcement authorities as they investigate this incident. Law enforcement authorities have not asked us to delay sending this notice to you because of their investigation. We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment card statements for unauthorized charges and monitoring free credit reports for fraudulent activity. If you suspect that an unauthorized charge has been placed on your account, you can report it to your payment card issuer. According to the payment card brands’ policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner. If you suspect that you may be the victim of identity theft, you should contact your local law enforcement, state attorney general, and/or the Federal Trade Commission.

0123456



We deeply regret that this incident occurred and apologize for any inconvenience it has caused you. If you have any questions about this incident, please do not hesitate to contact our customer care center at (888) 488-5978, visit our website www.searsholdings.com/update where we provide information regarding the incident and will post updates as necessary, or contact us by mail at 3333 Beverly Road, Hoffman Estates, IL 60179.

Sincerely,

Leena Munjal
Chief Digital Officer

ADDITIONAL RESOURCES, CREDIT ALERTS AND FREEZES

Information about Identity Theft

Federal Trade Commission

The Federal Trade Commission provides information about how to avoid identity theft, including information about placing fraud alerts and security freezes on your credit report.

- Visit: <http://www.ftc.gov/idtheft>
- Call (toll-free): 1-877-ID-THEFT (1-877-438-4338)
- Write: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

State Specific Information

Some states provide additional information and resources to assist their residents when there is a data security breach.

Information for Maryland Residents

For more information on identity theft, you can contact the Maryland Attorney General's Office:
Address: 200 St. Paul Place, Baltimore, MD 21202
Telephone: 1-410-576-6491
Website: www.oag.state.md.us/idtheft/index.htm.

Information for North Carolina Residents

For more information on identity theft, you can contact the North Carolina Attorney General's Office:
Address: 9001 Mail Service Center, Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
Fax: 1-919-716-6750
Website: <http://www.ncdoj.gov>

Free Annual Credit Reports

You may obtain a free copy of your credit report once every 12 months.

- Visit: <http://www.annualcreditreport.com>
- Call (toll-free): 1-877-322-8228
- Write: Complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the form at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>).

You also may purchase a copy of your credit report by contacting one of the three national consumer reporting agencies using the information below.

Equifax 1-800-525-6285 www.equifax.com P. O. Box 740241 Atlanta, GA 30374-0241	Experian 1-888-397-3742 www.experian.com P. O. Box 9554 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19022
---	---	---

0123456



D7052-L02

Fraud Alerts: “Initial Alert” and “Extended Alert”

You can place two types of fraud alerts on your credit report to put your creditors on notice that you may be a victim of fraud: an “Initial Alert” and an “Extended Alert.” An Initial Alert stays on your credit report for 90 days. You may ask that an Initial Alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit report for seven years. To obtain the Extended Alert, you must provide proof to the consumer reporting agency (usually in the form of a police report) that you actually have been a victim of identity theft. You have the right to obtain a police report regarding the data security incident. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three consumer reporting agencies provided above.

A potential drawback to activating a fraud alert would occur when you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. A fraud alert may interfere with or delay your ability to obtain credit.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. Fraud alerts can legally be ignored by creditors. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

To place a fraud alert on your credit report, you may contact all of the three major consumer reporting agencies using the information below that they have published. Consumer reporting agencies will need to verify your identity, which will require providing your Social Security number and other similar information.

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
<https://fraud.transunion.com>
1-800-680-7289

Equifax
P. O. Box 740241
Atlanta, GA 30374-0241
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
1-888-766-0008

Experian
P. O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
1-888-397-3742

Placing a fraud alert does not damage your credit or credit score. Additional information may be obtained from www.annualcreditreport.com.

Credit or Security Freeze on Credit File

In some U.S. states, you have the right to put a credit freeze (also known as a security freeze) on your credit file. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each consumer reporting agency.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit report, contact the consumer reporting agencies using the information below, and be prepared to provide the following (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well):

- (1) full name, with middle initial and any suffixes;
- (2) Social Security number;
- (3) date of birth;
- (4) current address and any previous addresses for the past two years; and
- (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of between \$5.00 and \$20.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

The addresses of consumer reporting agencies to which requests for a security freeze may be sent are:

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
<https://freeze.transunion.com>

Equifax
Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian
P. O. Box 9532
Allen, TX 75013
<https://www.experian.com/freeze/center.html>

The consumer reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

0123466



D7052-L02

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include:

- proper identification (name, address, and Social Security number);
- the PIN or password provided to you when you placed the security freeze; and
- the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

The consumer reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

* * *



3333 Beverly Rd
Hoffman Estates, IL 60179

April 25, 2018

D7052-L02-0123456 0001 00000001 *****MIXED AADC 159
SAMPLE A SAMPLE - GENERAL WITH APPENDIX



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Important Payment Card Security Notification.
Please read this entire letter.

Dear Sample A Sample,

Sears Holdings (“Sears”) was recently notified, by a vendor providing online support services on our websites at Sears.com and Kmart.com, that the vendor had experienced a security incident in which an unauthorized individual incorporated a malicious script into our vendor’s code which was used to provide certain services on our websites. The malicious script collected names, addresses, and payment card information. You are receiving this letter because our records show that information about your Card Type ending in ##### may have been affected by this incident.

As soon as our vendor informed us of this incident in mid-March, Sears notified the payment card companies to help prevent potential fraud, and conducted a thorough investigation of the incident. The investigation concluded that the incident affected some customers on Sears.com and Kmart.com who completed an online order between September 27, 2017 and October 12, 2017 and entered their payment card information manually on the checkout screen. Our vendor has assured us that it has taken steps to secure its systems and prevent this type of incident from occurring again in the future. There is no evidence that our stores were compromised or that any internal Sears systems were accessed by those responsible.

We are cooperating with law enforcement authorities as they investigate this incident. Law enforcement authorities have not asked us to delay sending this notice to you because of their investigation. We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment card statements for unauthorized charges and monitoring free credit reports for fraudulent activity. If you suspect that an unauthorized charge has been placed on your account, you can report it to your payment card issuer. According to the payment card brands’ policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner. If you suspect that you may be the victim of identity theft, you should contact your local law enforcement, state attorney general, and/or the Federal Trade Commission.

0123456



We deeply regret that this incident occurred and apologize for any inconvenience it has caused you. If you have any questions about this incident, please do not hesitate to contact our customer care center at (888) 488-5978, visit our website www.searsholdings.com/update where we provide information regarding the incident and will post updates as necessary, or contact us by mail at 3333 Beverly Road, Hoffman Estates, IL 60179.

Sincerely,

Leena Munjal
Chief Digital Officer

ADDITIONAL RESOURCES, CREDIT ALERTS AND FREEZES

Information about Identity Theft

Federal Trade Commission

The Federal Trade Commission provides information about how to avoid identity theft, including information about placing fraud alerts and security freezes on your credit report.

- Visit: <http://www.ftc.gov/idtheft>
- Call (toll-free): 1-877-ID-THEFT (1-877-438-4338)
- Write: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

State Specific Information

Some states provide additional information and resources to assist their residents when there is a data security breach.

Information for Maryland Residents

For more information on identity theft, you can contact the Maryland Attorney General's Office:
Address: 200 St. Paul Place, Baltimore, MD 21202
Telephone: 1-410-576-6491
Website: www.oag.state.md.us/idtheft/index.htm.

Information for North Carolina Residents

For more information on identity theft, you can contact the North Carolina Attorney General's Office:
Address: 9001 Mail Service Center, Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
Fax: 1-919-716-6750
Website: <http://www.ncdoj.gov>

Free Annual Credit Reports

You may obtain a free copy of your credit report once every 12 months.

- Visit: <http://www.annualcreditreport.com>
- Call (toll-free): 1-877-322-8228
- Write: Complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the form at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>).

You also may purchase a copy of your credit report by contacting one of the three national consumer reporting agencies using the information below.

Equifax 1-800-525-6285 www.equifax.com P. O. Box 740241 Atlanta, GA 30374-0241	Experian 1-888-397-3742 www.experian.com P. O. Box 9554 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19022
---	---	---

0123456



D7052-L02

Fraud Alerts: “Initial Alert” and “Extended Alert”

You can place two types of fraud alerts on your credit report to put your creditors on notice that you may be a victim of fraud: an “Initial Alert” and an “Extended Alert.” An Initial Alert stays on your credit report for 90 days. You may ask that an Initial Alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit report for seven years. To obtain the Extended Alert, you must provide proof to the consumer reporting agency (usually in the form of a police report) that you actually have been a victim of identity theft. You have the right to obtain a police report regarding the data security incident. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three consumer reporting agencies provided above.

A potential drawback to activating a fraud alert would occur when you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. A fraud alert may interfere with or delay your ability to obtain credit.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. Fraud alerts can legally be ignored by creditors. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

To place a fraud alert on your credit report, you may contact all of the three major consumer reporting agencies using the information below that they have published. Consumer reporting agencies will need to verify your identity, which will require providing your Social Security number and other similar information.

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
<https://fraud.transunion.com>
1-800-680-7289

Equifax
P. O. Box 740241
Atlanta, GA 30374-0241
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
1-888-766-0008

Experian
P. O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
1-888-397-3742

Placing a fraud alert does not damage your credit or credit score. Additional information may be obtained from www.annualcreditreport.com.

Credit or Security Freeze on Credit File

In some U.S. states, you have the right to put a credit freeze (also known as a security freeze) on your credit file. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each consumer reporting agency.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit report, contact the consumer reporting agencies using the information below, and be prepared to provide the following (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well):

- (1) full name, with middle initial and any suffixes;
- (2) Social Security number;
- (3) date of birth;
- (4) current address and any previous addresses for the past two years; and
- (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of between \$5.00 and \$20.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

The addresses of consumer reporting agencies to which requests for a security freeze may be sent are:

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
<https://freeze.transunion.com>

Equifax
Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian
P. O. Box 9532
Allen, TX 75013
<https://www.experian.com/freeze/center.html>

0123456



The consumer reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

D7052-L02

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include:

- proper identification (name, address, and Social Security number);
- the PIN or password provided to you when you placed the security freeze; and
- the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

The consumer reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

* * *