



Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

July 8, 2020

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Claire's Stores, Inc. ("Claire's"), to notify your office of a security incident involving Iowa residents.

Claire's began an investigation of its e-commerce websites after it was contacted by a security researcher the night of Thursday, June 11, 2020 who claimed to have determined that Claire's e-commerce site had been compromised. Claire's immediately took action to investigate the security researcher's claim and identified and removed unauthorized code in the code that operates its e-commerce site on Friday, June 12, 2020. The added code was capable of obtaining information entered by customers during the checkout process and sending it out of the Claire's system. A security firm was engaged, and Claire's identified the specific transactions involved. Claire's also reinforced the security of its site. Purchases made in Claire's retail store locations were not involved. Findings from the investigation show the code was first added on April 7, 2020. There were several times from April 7 to June 12, 2020 when the added code was not present because of new code deployments.

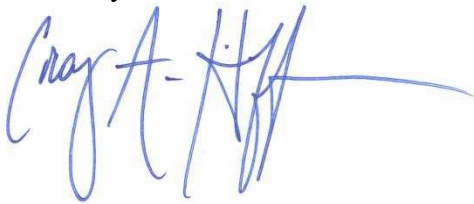
The information entered during the checkout process that could have been copied includes first and last name, address, email address (only if a customer chose to edit their email on the checkout page), phone number, payment card number, expiration date, and card verification code for payment cards used for transactions while the unauthorized code was present. Gift card number and PIN for gift cards used for transactions while the unauthorized code was present

could have also been copied. Also, if a customer created a Claire's account during the checkout process the account password, but not email address, may have been copied.

Beginning today, Claire's is notifying 591 Iowa residents via U.S. mail. A copy of the notification letter is enclosed.¹ The letter contains enrollment information for a complimentary one-year membership to Experian's® IdentityWorks internet surveillance and identity theft insurance. Claire's implemented additional security measures, notified the payment cards network, and notified law enforcement. Claire's is providing a telephone number for individuals to call with any questions they may have.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Craig A. Hoffman", with a long horizontal flourish extending to the right.

Craig A. Hoffman
Partner

Attachment

¹ This report does not waive Claire's' objection that Iowa lacks personal jurisdiction over the company related to this matter.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

<<b2b_text_1(SubjectLine)>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Claire's and Icing are writing to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?

We recently began an investigation of our e-commerce websites, and on June 12, 2020 we identified and removed computer code that had been added to our site by an unauthorized person. The added code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. A security firm was engaged and we identified the specific transactions involved. We also reinforced the security of our site. Purchases made in our retail store locations were not involved.

Findings from the investigation show the code was first added on April 7, 2020. There were several times from April 7 to June 12 when the added code was not present because of new code deployments. We are notifying you because you placed an order during a time the added code was present.

What Information Was Involved?

The information entered during the checkout process that could have been copied includes:

- **Contact information** - first and last name, address, email address (only if you chose to edit your email on the checkout page), and phone number.
- **Payment card information** - payment card number, expiration date, and card verification code for the payment card ending in <<b2b_text_2(Last4ofCard)>>. If you made more than one purchase between April 7 and June 12 and used more than one card, you can identify the other cards involved by looking at your email receipt or by calling us at the number below.
- **Other information** - if you paid with a gift card or created a Claire's account during the checkout process, the added code could have copied the gift card number and PIN or the account password (but not email address).

What We Are Doing.

Claire's conducted an investigation, implemented additional security measures, and hired resources to inform and assist our customers. We also notified the payment cards network so that they can inform the banks that issued the cards. Claire's also notified law enforcement and relevant authorities.

We are also offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with internet surveillance and identity theft insurance at no cost to you upon enrollment. To activate your membership and start monitoring your personal information please follow the steps on page 3.

What You Can Do.

We encourage you to closely review your payment card account statements for any unauthorized charges. You should immediately report any unauthorized charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any further questions or concerns, we established a dedicated call center, which can be reached by calling 1-844-951-2879, Monday through Friday from 9:00 a.m. – 6:30 p.m. EDT, excluding US holidays.

Sincerely,

A handwritten signature in black ink that reads "Marie Hodge". The signature is written in a cursive, flowing style.

Marie Hodge
Executive Director, Communications and Operations

Activate IdentityWorks Now in Three Easy Steps

1. ENROLL by: <<b2b_text_3(EnrollmentDeadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/identity>.
3. PROVIDE the **Activation Code**: <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 288-8057**. Be prepared to provide engagement number <<b2b_text_4(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

Once you enroll in Experian IdentityWorks, you will have access to the following benefits:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/identity>
or call (877) 288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **(877) 288-8057**.

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place fraud alerts in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.