

STATE OF NH
DEPT OF JUSTICE

2019 NOV 22 AM 11:10

BakerHostetler

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

November 21, 2019

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing on behalf of our client, Century 21 Department Stores, LLC ("Century 21"), to notify your office of a security incident involving the payment card information of New Hampshire residents.

Century 21 recently learned of suspicious activity involving the code for its website, c21stores.com. As soon as Century 21 became aware of this activity, it immediately commenced an investigation and discovered the presence of unauthorized code on the website. Century 21 immediately removed the code. A leading cybersecurity firm was then engaged to assist with Century 21's investigation. By November 5, 2019, it was determined that the code may have been present and capable of copying information entered by customers during the checkout process at certain, but not all, times during the general period of August 27, 2019 to October 10, 2019. The information that may have been collected by the code during the checkout process that could have potentially been copied includes the first and last names, addresses, telephone numbers, payment card numbers, payment card expiration dates, and card verification codes of two New Hampshire residents.

Beginning today, Century 21 notified the two New Hampshire residents via United States First Class mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A sample copy of the notification letter is attached. Century 21 has also established a dedicated call center that the individuals receiving notice can call with any questions regarding this incident. In addition, Century 21 has notified the payment card brands and is advising the individuals involved to review

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Attorney General Gordon MacDonald

November 21, 2019

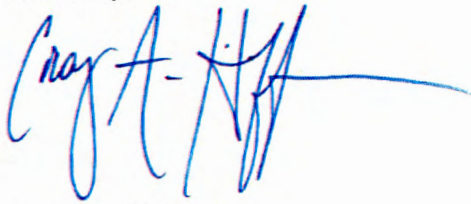
Page 2

their payment card statements and immediately report any unauthorized charges to the bank that issued their card.

In response to this incident, Century 21 has implemented a number of additional security measures, including multifactor authentication, and will continue to look for security enhancements to further protect customer information.

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

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

Enclosure



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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Century 21 Stores values the relationship we have with our customers and understands the importance of protecting your personal information. We are writing to inform you about an incident involving your payment card information. This letter is to provide information about the incident, measures that we have taken in response, and some additional steps you may consider taking.

WHAT HAPPENED.

We were recently alerted to suspicious activity involving the code for our website, c21stores.com. As soon as we became aware of this, we commenced an investigation and discovered the presence of unauthorized code on the website. We immediately removed the code. A leading cybersecurity firm was then engaged to assist with our investigation. By November 5, 2019, it was determined that the code may have been present and capable of copying information entered by customers during the checkout process at certain, but not all, times during the general period of August 27, 2019 to October 10, 2019. We are notifying you because you placed an order on our website during a timeframe when the code may have been present.

WHAT INFORMATION WAS INVOLVED.

The information that may have been collected during the checkout process that could have potentially been copied includes your first and last name, address, telephone number, payment card number, expiration date, and card verification code for your payment card(s) ending in <<b2b_text_1 (Last 4 of Card Number)>>.

WHAT WE ARE DOING.

In response to this incident, we have implemented a number of additional security measures, including multifactor authentication, and we will continue to look for security enhancements to protect customer information.

WHAT YOU CAN DO.

We advise you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information on additional steps you can take can be found on the following pages.

FOR MORE INFORMATION.

We deeply regret any inconvenience or concern this incident may cause you. If you have any remaining questions regarding this incident, please contact 1-888-918-0471, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Sebastian Lesage
Vice President, Digital

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

If you are a resident of Connecticut, Maryland, or North Carolina, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *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
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of 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 below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 (1) 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth

4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity 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 credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

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). Here is a summary of your major rights under FCRA. 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.