

Nicholas J. DiCesare
Partner

October 25, 2024

VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED AND EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: The Mick's in Cooperstown, Inc. d/b/a Mickey's Place:
Notice of Security Incident

Dear Office of the Attorney General:

We are writing on behalf of our client, The Mick's in Cooperstown, Inc. d/b/a Mickey's Place ("Mickey's Place"), to notify you of a recent breach of security incident involving computerized data that may have affected fifty-three (53) Maryland residents.

On September 2, 2024, Mickey's Place identified unusual information in its website's code. Immediately upon learning of the unusual code, Mickey's Place took steps to secure its website, and thereafter began an investigation with the assistance of an independent cybersecurity firm. Mickey's Place completed its investigation on September 20, 2024 where it was ultimately able to determine that the unauthorized code was inserted into its website on February 7, 2024, and that it was diverting information from credit card purchases conducted on the website to an outside source. Mickey's Place reviewed all transactions conducted through the website between February 7, 2024 and September 2, 2024 to identify individuals whose information could potentially have been impacted by this situation, and is providing notice to anyone who conducted a website transaction during that time period. This includes anyone who conducted a transaction on the website and provided their name, address, and credit card number (including expiration date and CVV code). Because of the unauthorized code on the website, that information may have been diverted to an unauthorized individual, though Mickey's investigation was not able to determine specifically whose information was diverted.

As part of its ongoing commitment to information security, Mickey's also reviewed its existing data security safeguards and procedures, and is continuing to educate its employees on best practices for data security. Mickey's Place underwent a password reset and added additional security monitoring so that they are alerted immediately if there is unusual activity or if code is added to its website. Mickey's Place also implemented multi-factor authentication. In addition,

October 25, 2024

Page 2

Mickey's Place has offered credit monitoring for 12 months through Equifax Credit Watch™ Gold (see Exhibit A for template notice).

If you have any questions regarding this submission or require additional information, kindly contact me. Thank you.

Very truly yours,

s/ Nicholas J. DiCesare

Nicholas J. DiCesare

NJD: bcs

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

<<Variable Data 1>>

Dear <<Full Name>>:

At Mickey's Place ("Mickey's"), we understand the importance of protecting and securing personal information that you provide when doing business with us. Regrettably, I am writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened? We recently completed an investigation involving the unauthorized access to Mickey's website. On September 2, 2024, Mickey's identified unusual information in its website's code. Immediately upon learning of the unusual code, Mickey's took steps to secure its website, and thereafter began an investigation with the assistance of an independent cybersecurity firm. Mickey's was ultimately able to determine that the unauthorized code was inserted into its website on February 7, 2024, and that it was diverting information from credit card purchases conducted on the website to an outside source. We have reviewed all transactions conducted through the website between February 7 and September 2 to identify individuals whose information could potentially have been impacted by this situation, and are providing this notice to you because you conducted a website transaction during that time period.

What Information Was Involved? After completing our investigation on September 20, 2024, we determined that you conducted a transaction on the website in relation to which you provided your name, address, and credit card number (including expiration date and CVV code). Because of the unauthorized code on the website, that information may have been diverted to an unauthorized individual, though our investigation was not able to determine specifically if your information was diverted.

What Is Mickey's Doing? Mickey's conducted a thorough investigation of its systems to ensure that the systems are secure and to attempt to identify the nature and potential scope of the unauthorized website access. As stated above, the investigation determined that an unauthorized individual was able to insert code to the website that diverted certain information, but found no evidence of unauthorized activity in any other system. As part of our ongoing commitment to information security, Mickey's also reviewed its existing data security safeguards and procedures, and is continuing to educate our employees on best practices for data security. We want to assure you that we take this incident and the security of your personal data very seriously.

What Can You Do? We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. In order to assist you, we have secured the services of Equifax to provide identity monitoring at no cost to you for <<CM Duration>>. Your identity monitoring services through Equifax's Credit Watch Gold program include credit file monitoring, webscan, and identity restoration service (among other things). For more information on identity theft prevention and the Equifax Credit Watch Gold service, including instructions on how to activate your complimentary <<CM Duration>> membership, please see the following page with enrollment instructions.



<<Full Name>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. If you have any questions, please call 855-277-4852, Monday through Friday from 9:00 A.M. through 9:00 P.M. Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'VR', with a stylized flourish at the end.

Vincent Russo
Owner

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 over the next 12 to 24 months. 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 your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

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. District of Columbia residents may also contact Barclay Damon at <<address>> / <<telephone number>>.

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. Maryland residents may also contact Barclay Damon at <<address>> / <<telephone number>>.

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 / 1-800-6971220, <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

Rhode Island: This incident involves <<RI Count>> individuals in Rhode Island. Under Rhode Island 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: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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.