



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

APR 15 2020

CONSUMER PROTECTION

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 10, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent TigerChef located at 27 Chestnut Street, Suffern, NY 10901 and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. TigerChef reserves the right to supplement this notice. By providing this notice, TigerChef does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 22, 2019, TigerChef[®] received notice that Visa identified 46 cards that may have been compromised as the result of being used on the TigerChef website. TigerChef immediately began an investigation. While the exact nature of the potential exposure could not be confirmed, TigerChef had discovered suspicious code on its checkout page on September 9, 2019. TigerChef had removed that code on September 10, 2019, and at that time there was no evidence of payment card compromise. However, it has been determined that this code may have captured card information. The unidentified code was on the checkout page of the TigerChef website beginning on July 17, 2019 until September 10, 2019, and any cards used during that time frame may be at risk. On January 3, 2020, TigerChef confirmed the identities of the individuals who made purchases during this time frame.

Office of the New Hampshire Attorney General

April 10, 2020

Page 2

The information that could have been subject to unauthorized access includes name, address, credit card information and username and password for the TigerChef website, if the user had one and entered it.

Notice to New Hampshire Residents

On or about April 10, 2020, TigerChef began to provide written notice to all affected individuals, which includes approximately three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

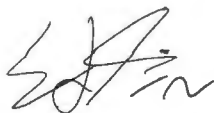
Upon discovering the event, TigerChef moved quickly to investigate and respond to the incident, assess the security of TigerChef systems, and notify potentially affected individuals. TigerChef has also implemented additional safeguards. TigerChef began monitoring the backend setting that had previously been changed. In addition, TigerChef implemented the iField framework, which adds extra layers of protection.

Additionally, TigerChef is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. TigerChef is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF; jcl
Enclosure

EXHIBIT A



Suburban Bowery of Suffern Inc dba TigerChef
27 Chestnut St
Suffern, NY 10901

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 10, 2020

<<Subject Line>>

Dear <<First Name>> <<Last Name>>,

TigerChef recently discovered an incident that may affect the security of some of your personal information. We write to provide you with information on the incident, steps TigerChef is taking in response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? On October 22, 2019, TigerChef received notice that Visa identified 46 cards that may have been compromised as the result of being used on the TigerChef website. TigerChef immediately began an investigation. While the exact nature of the potential exposure could not be confirmed, TigerChef had discovered suspicious code on its checkout page on September 9, 2019. TigerChef removed that code on September 10, 2019, and at that time there was no evidence of payment card compromise. However, it has been determined that this code may have captured card information. The unidentified code was on the checkout page of the TigerChef website beginning on July 17, 2019 until September 10, 2019, and any cards used during that time frame may be at risk. On January 3, 2020, TigerChef confirmed the identities of the individuals who made purchases during this time frame.

What Information Was Involved? We confirmed that you used a payment card on the TigerChef website during the window of compromise. As a result, information entered onto the site could have been captured. This may include your name and credit card information.

What We Are Doing. Information privacy and security are among our highest priorities. TigerChef has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems. TigerChef began monitoring the backend setting that had previously been changed. In addition, TigerChef implemented the iField framework, which adds extra layers of protection.

In an abundance of caution, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity. Please review the enclosed "Steps You Can Take to Protect Your Information" to learn more about ways to protect your personal information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact 1-833-968-1685 (toll free) Monday through Friday, 6 a.m. to 6 p.m.

TigerChef takes the privacy and security of personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

TigerChef

Steps You Can Take to Protect Your Personal Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.experian.com/freeze/center.html

www.transunion.com/credit-freeze

www.equifax.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.experian.com/fraud/center.html

www.transunion.com/fraud-victim-resource/place-fraud-alert

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, and www.ncdoj.gov. Individuals may obtain information from these sources about preventing identity theft.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.