



STATE OF NH
DEPT OF JUSTICE
10 APR 19 AM 9:56

FAMOUS DAVE'S OF AMERICA, INC.
12701 WHITEWATER DRIVE, SUITE 200
MINNETONKA, MN 55343

T 952-294-1300 famousdaves.com

April 16, 2010

Attorney General Michael J. Delaney
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

I am writing on behalf of Famous Dave's of America, Inc. ("Famous Dave's") to inform you of a security breach potentially affecting 2 New Hampshire residents. On the afternoon of March 21, a thief stole a piece of baggage and other personal items from the vehicle of a companion of a Famous Dave's employee. The baggage contained a laptop computer used by the employee for work. The employee immediately reported the theft to local law enforcement authorities. The investigation into the theft is on-going, and Famous Dave's is cooperating fully.

Famous Dave's has worked diligently to determine the identity of the individuals whose personal information may have been compromised by this theft. Famous Dave's has been able to determine that, as noted above, 2 individuals who reside in New Hampshire, may have been affected by the theft. Famous Dave's anticipates that it will mail the formal notice of security breach on or about April 16, 2010. A copy of the letter that will be sent to the affected New Hampshire resident is enclosed.

If you have any questions concerning the matters discussed above, please do not hesitate to call me at (952) 294-1276.

Sincerely,


Jackie Kane Ottoson
Vice President of Human Resources and Training

Enclosure



FAMOUS DAVE'S OF AMERICA, INC.
12701 WHITEWATER DRIVE, SUITE 200
MINNETONKA, MN 55343

T 952-294-1300 famousdaves.com

April 2, 2010

«First» «last»
«Address_1»
«City», «State» «ZIP»

Dear «First»:

Famous Dave's of America recognizes the importance of safeguarding its team members' personal information. To that end, the Company has implemented administrative, technical and physical safeguards for that information. Even the most rigorous safeguards, however, cannot guarantee protection against criminal conduct.

Our Company recently was the subject of such conduct, and we want to let you know that this criminal conduct could have a direct impact on you. On the afternoon of March 21, a thief stole a piece of baggage and other personal items from the vehicle of a companion of a Minnetonka-based team member. The baggage contained a laptop computer used by the team member for work. The team member immediately reported the theft to local law enforcement authorities. The investigation into the theft is on-going, and Famous Dave's is cooperating fully.

Since learning of the theft, Famous Dave's has worked diligently and on an expedited basis to reconstruct the information stored on the stolen laptop. Our investigation thus far indicates that the laptop contained a report with the first and last name and Social Security number (SSN) of Famous Dave's team members who were employed by the Company on or after November 1, 2009 and a few that left the company in 2008 and before November 1, 2009. The report contained similar personal information of former employees of the North Country group of restaurants located in the following New Jersey and New York locations: Brick Township, Hamilton (Mays Landing), Metuchen, Mountainside, New Brunswick, Smithtown and Westbury.

You are receiving this letter because Famous Dave's has reason to believe that you are one of individuals whose name and SSN were on the stolen laptop. We are relieved to report that the stolen laptop was password protected and did not contain credit or debit card numbers or financial account numbers.

In addition, neither the vehicle nor the stolen baggage would suggest to the perpetrator the nature of the information stored on the laptop. Consequently, we have no reason to believe that

the theft was directed at the information stored on the laptop. We also have received no reports to date indicating that the information stored on the laptop has been misused.

Famous Dave's regrets that this incident has occurred, and we apologize for any concerns or inconvenience it may cause you. In response to this incident, Famous Dave's will be taking immediate steps to determine how its policies and practices can be further enhanced to reduce the risk of a recurrence.

In addition, out of an abundance of caution and to lessen the potential inconvenience to you, we have arranged for **one year of credit monitoring through ConsumerInfo.com, Inc., an Experian® company, at no cost to you.** If you choose to enroll in the product membership, known as **TripleAlertSM**, you will enjoy the following benefits:

- Daily monitoring of your credit report at each of the three national credit bureaus;
- Notification of key changes that may help you to identify possible fraudulent activity;
- Monthly "no-hit" notifications if no key changes were detected on your credit reports;
- \$25,000 of identity theft insurance, provided by Virginia Surety, Inc.;
- If you are victimized by identity theft, a dedicated representative will provide you with fraud resolution services free of charge.

You can enroll on-line at **<http://partner.consumerinfo.com/famousdaves>** by entering the activation code provided below. You will be instructed on how to initiate your online membership. If you have any questions concerning TripleAlert, or concerning this incident, or if you prefer to enroll over the phone for delivery of your membership via US mail, please call Consumerinfo.com at **1-866-584-9681**. They have established representatives dedicated to responding to your questions about this incident and about the product membership.

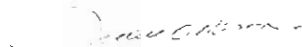
Your Credit Monitoring Activation Code is «Activation_Code»:

You must enroll by: **July 3, 2010**

In addition to arranging for one year of free credit monitoring, we have prepared the **Recommended Steps** enclosed with this letter. The enclosure provides you with additional information on how to protect yourself against the possibility of identity theft. Please review it carefully.

Again, Famous Dave's regrets that this incident occurred and is taking steps to reduce the inconvenience to you. If you have any questions, please call Consumerinfo.com's dedicated representatives at **1-866-584-9681**.

Sincerely,



Jackie Ottoson
Vice President of Human Resources and Training

Recommended Steps

By immediately taking the following steps, you can help reduce the risk that your personal information will be misused.

1. Activate the credit monitoring paid for by Famous Dave's. You must personally activate credit monitoring for it to be effective.

The Notification Letter included in this mailing will provide you with instructions and information to activate the TripleAlert membership. If you need assistance or to enroll by telephone, you can contact Experian directly at **1-866-584-9681**. With Experian's credit monitoring, you will receive:

- Automatic, daily monitoring of the Experian, Equifax and TransUnion credit files;
- Notification within 24 hours of critical changes to your credit report. You will quickly find out about changes, including potentially fraudulent activity such as new inquiries, new accounts, late payments, and more;
- Monthly "no-hit" notices, letting you know there were no changes with your credit activity;
- Toll-free access to fraud resolution specialists who help investigate each incident; contact credit grantors to dispute charges, close accounts and compile documents; and contact all relevant government agencies and law enforcement officials as needed;
- \$25,000 of identity theft insurance with zero deductible provided by Virginia Surety Company, Inc. for certain identity theft expenses.

Enrolling in TripleAlert will not affect your credit score.

2. Place a fraud alert with one of the three national credit bureaus.

You can place an initial fraud alert with one of the three national credit bureaus by phone and also via Experian's website. If you elect to participate in the credit monitoring as discussed in #1, above, please wait until **after** you have activated the credit monitoring before placing a fraud alert. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Experian Fraud Reporting
(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

You should contact only one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place an alert on their records as well. You will receive confirmation letters in the mail and will then be able to order a credit report from each of the three credit bureaus, free of charge, for your review. You also can ask the credit bureau for information on how to extend your initial fraud alert for seven (7) years.

You have the right under California law 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. You can request additional information and instructions for placing a credit freeze from any of the credit bureaus listed above.

3. Review your credit reports. You can receive free credit reports by placing a fraud alert and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

4. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers.

5. Respond to suspicious activity. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. If you receive an e-mail alert from Experian, contact an Experian fraud resolution representative at 1-866-584-9681. You also should consider notifying your local police department and the Federal Trade Commission of any suspicious activity involving your account statements or credit reports.

6. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
(877) IDTHEFT (438-4338)
TDD: (202) 326-2502

ADDITIONAL INFORMATION FOR MASSACHUSETTS RESIDENTS

You have the right under Massachusetts law to report this incident to the police located in the county where you reside and to receive a police incident report from that police department within twenty-four hours of filing the report.

You have the right under Massachusetts law to place a "security freeze" on your credit report with the national credit bureaus. A security freeze prohibits the consumer reporting agency, with limited exceptions, from releasing any information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent.

You can request a security freeze by sending written notice to each of the national credit bureaus at the addresses listed below. Your request must include the following information about you: (a) full name, with middle initial and generation, such as Jr., Sr., II, III, *etc.*; (b) Social Security number; (c) date of birth (month, day and year); (d) current address and previous addresses for the past two years; and (e) the \$5 fee or a valid police incident report. You can pay by personal check or by credit card. For credit card payment, you will need to provide the following information: (a) name of the person as it appears on the credit card; (b) type of credit card (*e.g.*, American Express, Mastercard, VISA, or Discover Card); (c) complete account number; (d) expiration data (month and year); (d) for American Express - 4 digit Card Identification Number (on front of card above the account number); for Mastercard, VISA, or Discover Card - 3 digit Card Identification Number (on back of card at the end of the account number).

You also must include one copy of a government-issued identification card, such as a driver's license, state or military ID card, *etc.*, and one copy of a utility bill, bank or insurance statement, *etc.* Each copy must be legible (enlarge if necessary), display your name and current mailing address, and the date of the statement (statement dates must be recent).

ADDITIONAL INFORMATION FOR MARYLAND RESIDENTS

You can contact Maryland's Office of Attorney General for more information about how to protect yourself against the possibility of identity theft as follows:

Consumer Protection Division
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Toll-free: 1-888-743-0023
Consumer complaint hotline: (410) 528-8662
Identity Theft Unit: idtheft@oag.state.md.us