Cooley

David J. Navetta
+1 720 566 4153
dnavetta@cooley.com

CONFIDENTIAL
Via E-Mail (consumer@iowa.gov)

March 29, 2019

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Earl Enterprises, to inform you of a data security incident potentially affecting payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants. Potentially affected restaurants include the following brands: Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria. While we cannot confirm the residency of the individuals potentially affected by the incident, some Iowa residents may have been affected. Earl Enterprises will be providing a notice for Iowa residents potentially affected by this incident, which will include some steps affected individuals may take to help protect themselves.

Upon learning of potential unauthorized access to certain payment cards, Earl Enterprises promptly launched an investigation and engaged two leading cyber security firms to assist in the company's review. As part of the investigation, Earl Enterprises has been in contact with federal law enforcement officials and is cooperating with them. Based on the investigation, it appears that unauthorized individuals installed malicious software on some point-of-sale systems at a certain number of Earl Enterprises' restaurants. The software was designed to capture payment card data, which could have included credit and debit card numbers, expiration dates and, in some cases, cardholder names. Although the dates of potentially affected transactions vary by location, guests that used their payment cards at potentially affected locations between May 23, 2018 and March 18, 2019 may have been affected by this incident. A full list of potentially affected restaurant locations is available at www.earlenterprise.com/incident.

The incident has now been contained, and Earl Enterprises is working diligently with security experts on further remediation efforts. Moving forward, the company will continue to closely monitor its systems and take additional security measures to help prevent something like this from happening again in the future. While Earl Enterprises has not discovered a breach with respect to any Iowa residents at this time, potentially affected residents are being notified beginning March 29, 2019 via notice on the websites of Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria, and through a media statement. The website notices and media statement refer guests to www.earlenterprise.com/incident, which webpage provides additional information about the incident, potentially affected locations and dates, a toll-free number where guests can call for additional

information, and steps that guests may take to help protect themselves. Copies of the notices are enclosed here for your reference.

Should you have any questions or concerns, please contact me at dnavetta@cooley.com or 720-566-4153.

Very truly yours,

David J. Navetta

DJN:ELL

Enclosures

201270732 v1

Earl Enterprises Notifies Guests of a Payment Card Incident

NEWS PROVIDED BY
Earl Enterprises →
Mar 29, 2019, 13:00 ET

ORLANDO, Fla., March 29, 2019 /PRNewswire/ -- Earl Enterprises recently became aware of a data security incident potentially affecting payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants. Potentially affected restaurants include the following brands: Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria. Once the company learned of the incident, the company promptly initiated an internal investigation and engaged two leading cybersecurity firms. As part of the investigation, the company has been in contact with federal law enforcement officials and is cooperating with them.

The security and privacy of guests' payment card data is a top priority, and the company deeply regrets that this incident occurred. The incident has now been contained, and Earl Enterprises is working diligently with security experts on further remediation efforts. Moving forward, the company will continue to closely monitor its systems and take additional security measures to help prevent something like this from happening again in the future.

Based on the investigation, it appears that unauthorized individuals installed malicious software on some point-of-sale systems at a certain number of Earl Enterprises' restaurants. The software was designed to capture payment card data, which could have included credit and debit card numbers, expiration dates and, in some cases, cardholder names. Although the dates of potentially affected transactions vary by location, guests that used their payment cards

at potentially affected locations between May 23, 2018 and March 18, 2019 may have been affected by this incident. Online orders paid for online through third-party applications or platforms were not affected by this incident.

A full list of potentially affected restaurant locations is available at www.earlenterprise.com/incident. The company advises all customers to visit this website to determine if they may have dined at one of the potentially affected restaurants.

As a best practice, it is always advisable for individuals to remain vigilant and monitor their payment card statements for suspicious charges or activity they do not recognize. If a guest suspects an unauthorized charge, they should immediately notify the bank that issued the card.

The company has set up a website at www.earlenterprise.com/incident with additional information and steps that guests can take to help protect themselves. A dedicated call center is also available for guests by calling 888-437-2399, toll-free, between 10 a.m. – 6 p.m. Eastern Time on Saturday, March 30, 2019 and Sunday, March 31, 2019, and between 9 a.m. – 9 p.m. Eastern Time, Monday through Friday (except holidays).

ABOUT EARL ENTERPRISES

Earl Enterprises is a recognized leader in the hospitality industry; building innovative, sustainable brands that guests can enjoy today and in the future, including restaurant brands Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria.

Media contact:
asadowsky@earlenterprise.com

SOURCE Earl Enterprises

Related Links

http://www.earlenterprise.com

NOTICE OF DATA BREACH

March 29, 2019

Earl Enterprises recently became aware of a data security incident potentially affecting payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants. Potentially affected restaurants include the following brands: Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria. We are providing this notice to our guests to inform them of the incident and steps they can take to help protect themselves. The security and privacy of our guests' payment card data is a top priority, and Earl Enterprises deeply regrets that this incident occurred.

What Happened

Once we learned of a potential incident, we promptly launched an internal investigation and engaged two leading cybersecurity firms. As part of the investigation, we have been in contact with federal law enforcement officials and are cooperating with them. Based on the investigation, it appears that unauthorized individuals installed malicious software on some point-of-sale systems at a certain number of Earl Enterprises' restaurants. A full list of potentially affected restaurant locations is available **below**.

What Information Was Involved

The malicious software was designed to capture payment card data, which could have included credit and debit card numbers, expiration dates and, in some cases, cardholder names. Although the dates of potentially affected transactions vary by location, guests that used their payment cards at potentially affected locations between May 23, 2018 and March 18, 2019 may have been affected by this incident. Online orders paid for online through third-party applications or platforms were not affected by this incident.

What We Are Doing

The incident has now been contained, and Earl Enterprises is continuing to work diligently with security experts on further remediation efforts. Moving forward, the company will continue to closely monitor its systems and take additional security measures to help prevent something like this from happening again in the future.

What You Can Do

You can carefully review credit and debit card account statements as soon as possible for suspicious charges or activity you do not recognize. As a best practice, we urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Guests can also review the "Information about Identity Theft Protection" reference guide, included **below** which describes additional steps that you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

Guests may obtain additional information by calling our dedicated call center toll-free at 888-437-2399 between 10 a.m. – 6 p.m. Eastern Time on Saturday, March 30, 2019 and Sunday, March 31, 2019, and between 9 a.m. – 9 p.m. Eastern Time, Monday through Friday (except holidays). You can also review FAQs, included **below**.

POTENTIALLY AFFECTED RESTAURANTS

Please use the below drop-down menus to identify potential affected restaurants:

Select A State ▾

Select A City ▾

Select A Concept ▾

INFORMATION ABOUT IDENTITY THEFT PROTECTION

REVIEW ACCOUNTS AND CREDIT REPORTS:

You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division,

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Security Freezes and Fraud Alerts: 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. 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the

victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of

removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- the unique personal identification number, password or similar device provided by the consumer reporting agency;
- proper identification to verify your identity;
- information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1,

2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit **https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf**, **https://www.consumerfinance.gov/learnmore/**, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

NATIONAL CREDIT REPORTING AGENCIES CONTACT INFORMATION

Equifax (www.equifax.com)

General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348
P.O. Box 2002

Experian (www.experian.com)

General Contact:
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact, Fraud Alerts and Security Freezes:

P.O. Box 2000
Chester, PA 19022
888-909-8872

FREQUENTLY ASKED QUESTIONS

1. **What happened?**

   Earl Enterprises recently became aware of a data security incident potentially affecting payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants. Once we learned of the incident, we promptly initiated an internal investigation and engaged two leading cybersecurity firms. The incident has now been contained, and the company continues to work diligently with security experts on further remediation efforts. As part of the investigation, we have been in contact with federal law enforcement officials and are cooperating with them. We remain committed to safeguarding the security of our guests' information and deeply regret that this incident occurred.

2. **Which of your restaurant brands may have been affected?**

   Potentially affected restaurants include the following brands: Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology and Tequila Taqueria.

3. **What brands were not affected?**

   Bertucci's, Seaside on the Pier and Café Hollywood.

4. **Were Planet Hollywood hotels and resorts affected?**

   No. This incident only affected certain restaurant locations.

5. **I purchased merchandise from a Planet Hollywood store – was I affected?**

   No. This incident only affected certain restaurant locations. A full list of potentially affected restaurant locations is available **above**.

6. **Were locations outside of the United States affected?**

   No, locations outside of the United States were not affected.

7. **What information was affected?**

   This incident may affect payment card information of a limited number of guests that dined at certain of Earl Enterprises' restaurants. Payment card information could have included credit and debit card numbers, expiration dates and, in some cases, cardholder names.

8. **When did this occur?**

   The dates of potentially affected transactions vary by location, but guests that used their payment cards at potentially affected locations between May 23, 2018 and March 18, 2019 may have been affected by this incident. A full list of potentially affected restaurant locations is available **above**.

9. **Were online orders affected?**

   No, online orders paid for online through third-party applications or platforms were not affected by this incident.

10. **What should I do?**

    Carefully review credit and debit card account statements as soon as possible for suspicious charges or activity you do not recognize. As a best practice, we urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card.

    For additional resources and information about preventing identity theft, you can review the Information About Identity Theft Protection guide, available **here**.

11. **There are fraudulent charges on my credit/debit card. What do I do?**

    Contact the bank or financial institution that issues your card right away and let them know of the fraudulent charges. The number to call is usually on the back of the card. They will provide you with instructions on how to dispute the charges. In instances of payment card fraud, it is important to note that

cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.