BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

December 31, 2019

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir or Madam:

Landry's takes the security of payment card data very seriously. Years ago (beginning in 2016), Landry's installed a payment processing solution that uses end-to-end encryption technology at all Landry's owned locations. Landry's is notifying customers by posting notice on its website and issuing a press release of an incident that was recently identified and addressed involving payment cards that, in rare circumstances, appear to have been mistakenly swiped by waitstaff on devices used to enter kitchen and bar orders, which are different devices than the point-of-sale terminals used for payment processing.

Landry's recently detected unauthorized access to the network that supports its payment processing systems for restaurants and food and beverage outlets. Landry's immediately launched an investigation, and a leading cybersecurity firm was engaged to assist. Although the investigation identified the operation of malware designed to access payment card data from cards used in person on systems at Landry's restaurants and food and beverage outlets, the end-to-end encryption technology on point-of-sale terminals, which makes card data unreadable, was working as designed and prevented the malware from accessing payment card data when cards were used on these encryption devices. Besides the encryption devices used to process payment cards, restaurants and food and beverage outlets also have systems that have a card reader attached for waitstaff to enter kitchen and bar orders and to swipe Landry's Select Club reward cards.

On November 22, 2019, Landry's first became aware of rare instances of unencrypted payment card data that may have been accessed by the malware. Landry's then worked diligently

to determine how the unencrypted card data may have entered the environment, the scope of the issue, and sought assistance from its payment processor and encryption-to-end encryption technology provider. The investigation determined that in rare circumstances, it appears waitstaff may have mistakenly swiped payment cards on the order-entry systems. The payment cards potentially involved in this incident are the cards mistakenly swiped on the order-entry systems.

The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card after it was swiped on the order-entry systems. In some instances, the malware only identified the part of the magnetic stripe that contained payment card information without the cardholder name. The general timeframe when data from cards mistakenly swiped on the order-entry systems may have been accessed is March 13, 2019 to October 17, 2019. At a small number of locations, access may have occurred as early as January 18, 2019. A full list of Landry's owned restaurants and food and beverage outlets is available on Landry's website.

Landry's does not have sufficient information to determine the name and mailing addresses of individuals whose payment card may have been mistakenly swiped on the order-entry systems during the relevant timeframe. Landry's, therefore, is unable to identify the number of Washington residents whose card may have been involved. Therefore, pursuant to Wash. Rev. Code § 19.255.010, Landry's is providing substitute notification to Washington residents whose card may have been mistakenly swiped on the order-entry systems at a Landry's location by issuing a press release and posting a statement on its website today, December 31, 2019. A copy of the press release and website message are enclosed. A list of all Landry's locations is available on the Landry's website. Landry's also established a dedicated call center that customers can call with related questions. Notification is being provided without unreasonable delay.

Landry's has removed the malware, implemented enhanced security measures, and is providing additional training to waitstaff. In addition, Landry's continues to support law enforcement's investigation.

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

Sincerely,

William R. Daugherty
Partner

Enclosure

Notice of Payment Card Incident

HOUSTON, Dec. 31, 2019 /PRNewswire/ -- Landry's, Inc. ("Landry's") takes the security of payment card data very seriously. Years ago (beginning in 2016), Landry's installed a payment processing solution that uses end-to-end encryption technology at all Landry's owned locations.

Landry's is notifying customers of an incident that it recently identified and addressed involving payment cards that, in rare circumstances, appear to have been mistakenly swiped by waitstaff on devices used to enter kitchen and bar orders, which are different devices than the point-of-sale terminals used for payment processing. This notice explains the incident, measures Landry's has taken, and some steps customers can take in response.

Landry's recently detected unauthorized access to the network that supports its payment processing systems for restaurants and food and beverage outlets. Landry's immediately launched an investigation, and a leading cybersecurity firm was engaged to assist. Although the investigation identified the operation of malware designed to access payment card data from cards used in person on systems at its restaurants and food and beverage outlets, the end-to-end encryption technology on point-of-sale terminals, which makes card data unreadable, was working as designed and prevented the malware from accessing payment card data when cards were used on these encryption devices. Besides the encryption devices used to process payment cards, Landry's restaurants and food and beverage outlets also have order-entry systems with a card reader attached for waitstaff to enter kitchen and bar orders and to swipe Landry's Select Club reward cards. In rare circumstances, it appears waitstaff may have mistakenly swiped payment cards on the order-entry systems. The payment cards potentially involved in this incident are the cards mistakenly swiped on the order-entry systems. Landry's Select Club rewards cards were not involved.

The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card after it was swiped on the order-entry systems. In some instances, the malware only identified the part of the magnetic stripe that contained payment card information without the cardholder name. The general timeframe when data from cards mistakenly swiped on the order-entry systems may have been accessed is March 13, 2019 to October 17, 2019. At a small number of locations, access may have occurred as early as January 18, 2019. A full list of Landry's owned restaurants and food and beverage outlets involved is available at https://www.landrysinc.com/CreditNotice/.

It is always advisable for customers to closely monitor their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to the financial institution that issued the card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

During the investigation, Landry's removed the malware and implemented enhanced security measures, and Landry's is providing additional training to waitstaff. In addition, Landry's continue to support law enforcement's investigation.

For more information regarding this incident, customers may visit https://www.landrysinc.com/CreditNotice/.

CONTACT: Katelyn Gosslee, Email: katelyn@dpwpr.com, Phone: 713-224-9115.

Payment Card Incident Notice

California Residents Click Here

Notice Of Payment Card Incident

Landry's, Inc. ("Landry's") takes the security of payment card data very seriously. Years ago (beginning in 2016), Landry's installed a payment processing solution that uses end-to-end encryption technology at all Landry's owned locations.

We are notifying customers of an incident that we recently identified and addressed involving payment cards that, in rare circumstances, appear to have been mistakenly swiped by waitstaff on devices used to enter kitchen and bar orders, which are different devices than the point-of-sale terminals used for payment processing. This notice explains the incident, measures we have taken, and some steps you can take in response.

Landry's recently detected unauthorized access to the network that supports our payment processing systems for restaurants and food and beverage outlets. We immediately launched an investigation, and a leading cybersecurity firm was engaged to assist. Although the investigation identified the operation of malware designed to access payment card data from cards used in person on systems at our restaurants and food and beverage outlets, the end-to-end encryption technology on point-of-sale terminals, which makes card data unreadable, was working as designed and prevented the malware from accessing payment card data when cards were used on these encryption devices. Besides the encryption devices used to process payment cards, our restaurants and food and beverage outlets also have order-entry systems with a card reader attached for waitstaff to enter kitchen and bar orders and to swipe Landry's Select Club reward cards. In rare circumstances, it appears waitstaff may have mistakenly swiped payment cards on the order-entry systems. The payment cards potentially involved in this incident are the cards mistakenly swiped on the order-entry systems. Landry's Select Club rewards cards were not involved.

The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card after it was swiped on the order-entry systems. In some instances, the malware only identified the part of the magnetic stripe that contained payment card information without the cardholder name. The general timeframe when data from cards mistakenly swiped on the order-entry systems may have been accessed is March 13, 2019 to October 17, 2019. At a small number of locations, access may have occurred as early as January 18, 2019. A full list of Landry's owned restaurants and food and beverage outlets involved is available here.

It is always advisable for individuals to closely monitor their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to the financial institution that issued the card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card. Please see the section that follows this notice for additional steps you may take.

During the investigation, we removed the malware and implemented enhanced security measures, and we are providing additional training to waitstaff. In addition, we continue to support law enforcement's investigation.

If you have any questions, please call 833-991-1538 from 8:00 a.m. to 8:00 p.m. CT, Monday through Friday. (The call center will be closed on New Year's Day).

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 you are a resident of Connecticut, Maryland, Massachusetts, New York, North Carolina, or Rhode Island, 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

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection

New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/

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 Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or 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 (see Credit Freeze section, below).

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 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.

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.