

16777



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Lee Auto Malls respects the privacy of your information, which is why we are writing to tell you about a data security incident by PaperlessPay Corporation ("PaperlessPay"), the company we use to provide your weekly pay stub information and produce electronic W-2's each year, that may have exposed some of your personal information on February 18, 2020.

When we learned about this incident on March 20, 2020, we contacted PaperlessPay to determine the nature and scope of its data event, including any potentially impacted individuals. After careful consideration of the information provided by PaperlessPay about a compromise to its information technology environment, we determined notice to you with an offer of two (2) years of identity monitoring without cost was appropriate.

What Information Was Involved

As a result of PaperlessPay's security incident, an unauthorized individual or individuals may have accessed or acquired some of your personal information, which may have included your first and last name, address, pay and withholdings, and Social Security number. Although we are unaware of any actual access to or acquisition of your personal information and have no evidence of any attempted or actual misuse of your information, we are providing you with notice of this event, our response, and steps you may take to protect against the possibility of identity theft and fraud.

What We Are Doing

To help relieve concerns following this incident, we have secured TransUnion to provide identity monitoring at no cost to you for two (2) years. TransUnion is an industry leader and functions as a first point of contact for credit-related issues, which allows it to efficiently furnish timely notification about credit-related issues to individuals enrolled in its identity monitoring service.

Visit www.MyTrueIdentity.com to activate and take advantage of your identity monitoring service.

You have until <<EnrollmentDate>> to activate your identity monitoring service.

myTrueIdentity Credit Monitoring Service Activation Code: <<ACTIVATION CODE>>

To receive credit services by mail instead of online, please call 1-855-288-5422. Additional information describing these services is included with this letter. We encourage you to review the description and to consider enrolling in the offered services.

Rest assured that we are committed to ensuring that PaperlessPay is keeping our data as secure as possible. PaperlessPay has represented to Lee Auto Malls that they have taken additional steps to further secure their environment as a result of this incident, and we will continue to monitor and evaluate their efforts to assure the continued security of your information.

What Else Can I Do To Protect My Information

We recommend that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit 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:

Equifax

P.O. Box 740241
Atlanta, Georgia 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 9554
Allen, Texas 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's, Equifax's or Transunion's websites. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

If you wish to place a fraud alert, contact any one of the credit bureaus using the contact information below:

Equifax Fraud Alert

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian Fraud Alert

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion Fraud Alert

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Security Freezes: You have the right to place a security freeze on your credit report free of charge. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified, or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card; (7) Social Security card, pay stub, or W2; and (8) any applicable incident report or complaint with a law enforcement agency. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You may obtain a security freeze from each of the three credit bureaus by written request, through the telephone, or by accessing their websites, using the contact information below:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
www.equifax.com/personal/credit-report-services

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their websites, or by phone, using the contact information above. You must provide proper identification (including name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their websites, or by phone (using the contact information above). You must provide proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338). IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

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 the Attorney General's office in your state. You can also obtain information from these sources about additional methods to prevent identity theft, and you can obtain information from the Federal Trade Commission and the consumer reporting agencies for more information regarding fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
1-877-438-4338
www.ftc.gov/idtheft

State Attorney General's Office Contact Information. For Massachusetts residents: You may contact the Attorney General, 1 Ashburton Place, Boston, MA 02108, <https://www.mass.gov/orgs/office-of-attorney-general-maura-healey>, 1-617-727-8400.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For More Information

For further information, please call 855-907-2080 between 9:00 a.m. and 9:00 p.m. EST. We take the protection of your personal information very seriously and apologize for any inconvenience PaperlessPay's incident may cause you. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Vicki Mann

Vicki Mann
CFO, Lee Auto Malls



Activation Code: <<Activation Code>>

Complimentary Two-Year *myTrueIdentity* 3B Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,[®] Experian,[®] and Equifax,[®] including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Joshua Brian

From: mhanson@leeautomall.com
Sent: Monday, March 23, 2020 8:53 AM
To: 'Vicki Mann'
Subject: FW: Followup on Feb 20, 2020 Email

Info on the breach

From: mark.broughton@paperlesspaycorp.com [mailto:mark.broughton@paperlesspaycorp.com]
Sent: Friday, March 20, 2020 5:17 PM
To: mhanson@leeautomall.com
Subject: Followup on Feb 20, 2020 Email



March 20, 2020

Electronic version sent to: mhanson@leeautomall.com

LeeAutoMall
c/o Magan Hanson
my-estub Administrator
777 CENTER STREET
P O BOX 297
AUBURN, ME 04210-0297

Re: Notice of Security Incident

Dear Magan:

I am writing in follow up to the email I sent to our clients on February 20, 2020 about the recent data security incident at PaperlessPay Corporation ("PaperlessPay"). Since then, we have worked diligently to investigate the incident and we are now able to provide this summary report as promised in my email. As a third-party agent that maintains data on your behalf, we take this incident and the security of your data seriously.

What Happened?

On February 19, 2020, the Department of Homeland Security ("DHS") contacted PaperlessPay and notified us that an unknown person was purporting to sell "access" to our client database on the dark web. In response, we shut down our web server and SQL server to prevent any potential unauthorized access. This interrupted our services to you and prevented your employees from accessing their payroll records for a short amount of time while the servers were offline.

Over the following weeks, we cooperated with the joint investigation conducted by DHS and the Federal Bureau of Investigation ("FBI"). Their investigation is ongoing, and we will continue to cooperate and help in any way we can. In addition, we retained the cybersecurity firm Ankura to help with our own, internal forensic investigation of the incident.

Through these investigations, we confirmed that an unknown person did gain access to our SQL server where your employees' data is stored on February 18, 2020. The available evidence has not, however, allowed DHS, the FBI, or Ankura to determine what data the person may have accessed or viewed while connected to the SQL server. It is possible the person only used his access to determine the size of the SQL database and to stage it for subsequent access that he could sell to others, and that he did not directly access any employee data himself. However, he would have had the capability to run queries against the SQL database and view its data, so we cannot rule out the possibility of unauthorized access.

Page 2 of 2

What information was involved?

The information stored in our SQL server about your employees consists of the data components that appear on their pay stubs and tax forms, including their name, address, pay and withholdings, last four digits of bank account number (if your company includes that information on its pay stubs), and Social Security number. However, these data components are stored on the SQL server in different tables that are associated by user ID numbers, not names, within each table. Therefore, the only way to associate any data with an individual would be to run a query against the database and have it aggregate an individual's name with his or her other data components.

What we are doing

In our capacity as a third-party agent that stores this employee data on your behalf, we are providing this supplemental notification, in addition to the one provided on February 24, to allow you to make any decisions about notification to your employees. We are committed to providing you with the information you need, so please contact us if you have other questions.

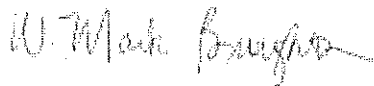
In the meantime, we have acted to secure our network and prevent future incidents. To resume our services, PaperlessPay rebuilt an entirely new domain controller, a new web server, and a new SQL server from scratch. We then restored database files to the new SQL server from backups. We assigned new IP addresses to all the new servers, changed all passwords for users and administrators, implemented a setting that requires clients to change their passwords when they login for the first time, and disabled all remote access capabilities to the new web server and SQL server.

We also installed an endpoint detection and response (EDR) application called Carbon Black on the new servers and other endpoints within our network. This has allowed us to monitor all activity while we completed this investigation of the incident. To date since Carbon Black has been running, there have been no indicators of compromise detected in the newly rebuilt environment, and we are pleased to report that all customer services are functioning as normal.

For more information

We are sorry for any concern or inconvenience this incident has caused or may cause you. For more information, please contact us at (800) 489-1711 ext. 422 or questions@paperlesspaycorp.com.

Sincerely,

A handwritten signature in dark ink, appearing to read "W. Mark Broughton". The signature is fluid and cursive, with the first name "W. Mark" and last name "Broughton" clearly distinguishable.

W. Mark Broughton
CEO

This email message is intended only for the addressee(s) and contains information that may be confidential. If you are not the intended recipient please notify the sender by reply email and delete this email. Use, disclosure or reproduction of this email by anyone other than the intended recipient(s) is strictly prohibited.