LEWIS BRISBOIS BISGAARD & SMITH LLP

STATE O
PT OF JUS
Y-3 PM 12:27

October 30, 2014

File No.
34467.56

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Supplemental Notice of Data Security Event

Dear Attorney General Foster:

We represent Delaware River & Bay Authority ("the Authority"), P.O. Box 71, New Castle, Delaware, 19720. On October 17, 2014, we provided notice to your office of an incident potentially affecting the security of the personal information of New Hampshire residents. A copy of our October 17, 2014 notice to you is attached to this letter as ***Exhibit A***.

On October 24, 2014, the independent third-party forensic experts assisting the Authority with its response to this data security event confirmed that credit and debit card data processed on certain card processing devices/systems relating to food, beverage, and retail sales at Cape May-Lewes Ferry's terminals and vessels were at risk from September 20, 2013 through August 7, 2014. To date, the forensic experts have not identified New Hampshire residents affected by this event. However, because certain food, beverage, and retail card processing devices/systems at Cape May-Lewes Ferry's terminals and vessels were at risk, the Authority notified the public of this data security event.

The Authority's notice to the public was distributed by a press release and a statement posted on the Cape May-Lewes Ferry's dedicated website http://cmlf.com/notification. A copy of this statement is attached as ***Exhibit B***. While the Authority has reason to believe that the intruder stole some data from certain credit and debit cards that were used during specified time frames at Cape May-Lewes Ferry's terminals and vessels, the Authority has not determined which specific cardholder's credit and debit card data may have been stolen by the intruder. Further, the Authority does not have sufficient contact information

for customers who may potentially be affected by this incident. The Authority therefore notified potentially affected customers by providing notice of this incident to major statewide media on October 24, 2014 in substantially the same form as the statement attached here as ***Exhibit C***. This statement was also posted on Cape May-Lewes Ferry's dedicated website, http://cmlf.com/notification, beginning on October 24, 2014.

The Authority takes this matter, and the security of the personal information in its care, seriously and continues to take measures to reduce the likelihood of this type of incident from occurring in the future. Upon discovery of this incident, the Authority immediately took steps to identify potential vulnerabilities with its systems including running scans of all credit card processing systems potentially affected by this matter. The Authority worked with the vendor who installed and performs maintenance on these systems to remove identified malware from affected credit card processing devices. The Authority is also taking steps to enhance the security of the food, beverage, and retail card processing devices/systems at Cape May-Lewes Ferry including replacing hard drives of registers processing payment card information, installing new antivirus protection, and updating policies and procedures regarding system access.

Should you have any questions regarding this [redacted]

Very truly yours,

[redacted]

JEP:mj

EXHIBIT A

LEWIS BRISBOIS BISGAARD & SMITH LLP

October 17, 2014

File No. 34467.56

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: *Preliminary* Notice of Data Security Event

Dear Attorney General Foster:

We represent Delaware River & Bay Authority ("the Authority"),P.O. Box 71, New Castle, Delaware, 19720, and are writing to notify you of a data security incident that may have compromised the security of personal information of New Hampshire residents. The Authority's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Authority does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On July 30, 2014, the Authority's credit card processor, Fifth Third Bank, alerted the Authority to a possible security compromise involving credit and debit card data utilized at Cape May-Lewes Ferry's terminals and vessels. An investigation into this incident was immediately initiated. The Authority's team, including third-party forensics experts, has been working continuously to understand the nature and scope of the incident. This investigation is ongoing. The security compromise, however, has been contained, and the Authority has been processing credit and debit card data at Cape May-Lewes Ferry's terminals and vessels securely since August 8, 2014.

Working with two independent third-party forensic experts, the Authority determined that *only* the security of certain card processing devices/systems relating to food, retail and

beverage sales at Cape May-Lewes Ferry's terminals and vessels were compromised. The Authority has reason to believe that certain credit and debit card data used between September 20, 2013 and August 7, 2014 at Cape May-Lewes Ferry's terminals and vessels may be at risk. Although the investigation is ongoing, the Authority has determined that information potentially affected by this data security event includes card numbers, the cardholder names, and/or the cards expiration date. To date, the forensic investigators have not identified New Hampshire residents affected by this event. However, if the investigation reveals that New Hampshire residents were affected by this event, notice will be provided pursuant to New Hampshire's data breach notification laws.

Other Steps Taken and To Be Taken

The Authority takes this matter, and the security of the personal information in its care, seriously and has taken measures to reduce the likelihood of this type of incident from occurring in the future. Upon discovery of this incident, the Authority immediately took steps to identify potential vulnerabilities with its systems including running scans of all credit card processing systems potentially affected by this matter. The Authority worked with the vendor who installed and performs maintenance on these systems to remove identified malware from affected credit card processing devices. The Authority engaged two independent third party forensic experts to assist in determining the nature and scope of this incident, and to assist in remediation. The Authority continues to work closely with these experts.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, [redacted].

[redacted]

James E[redacted]

JEP:mj

EXHIBIT B

Notice of Data Security Event

New Castle, Delaware, October 24, 2014 - On July 30, 2014, Delaware River and Bay Authority ("the Authority") was notified of a possible security compromise involving credit and debit card data stored on certain systems at the Cape May-Lewes Ferry's terminals and vessels. An investigation into this incident was immediately initiated and our team, including third-party forensics experts, has been working continuously to understand the nature and scope of the incident. Although this investigation is ongoing, we have determined that the security of card processing systems relating to food, beverage, and retail sales at the Cape May - Lewes Ferry were compromised and some data from certain credit and debit cards that were used from September 20, 2013 to August 7, 2014 at Cape May - Lewes Ferry's terminals and vessels may be at risk. The credit and debit card data potentially at risk includes the card number, the cardholder's name and/or the card's expiration date. We have not determined that any *specific* cardholder's credit or debit card data was stolen by the intruder.

"We take the security of our customers' personal information very seriously and work extremely hard to protect their credit and debit card data," said Heath Gehrke, Director of Ferry Operations. "Despite any company's best efforts, intrusions can occur. With the help of professional experts, we want to understand the nature and scope of this incident so we can learn from it." The Authority is also working with these experts to enhance the security of its credit and debit card processing systems at the Cape May-Lewes Ferry's terminals and vessels. Gehrke emphasized that the food, beverage, and retail locations at the Cape May - Lewes's terminals and vessels have been processing credit and debit card transactions securely since August 8, 2014. Gehrke also stressed that only food, beverage, and retail sales locations were affected by the security compromise. The Cape May - Lewes Ferry reservation system, including on-line bookings and terminal point-of-sale locations, utilized for the purchase of vehicle or passenger tickets was not compromised.

Please visit http://cmlf.com/notification to learn more about this data security event and the identity protection services being provided for potentially affected customers.

The Authority encourages its customers to remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, Cape May-Lewes Ferry customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069,

800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State Attorneys General may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

We regret any inconvenience this security compromise may have caused our customers. To better assist our customers whose card data may potentially have been affected, Cape May-Lewes Ferry has established a confidential hotline to answer questions. This hotline is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. C.S.T. and can be reached at 1-855-865-4457. Customers can also visit http://cmlf.com/notification for additional information.

EXHIBIT C

Notice of Data Security Event

[state], October 24, 2014 - On July 30, 2014, Delaware River and Bay Authority ("the Authority") was notified of a possible security compromise involving credit and debit card data stored on certain systems at the Cape May-Lewes Ferry's terminals and vessels. An investigation into this incident was immediately initiated and our team, including third-party forensics experts, has been working continuously to understand the nature and scope of the incident. Although this investigation is ongoing, we have determined that the security of card processing systems relating to food, beverage, and retail sales at the Cape May - Lewes Ferry were compromised and some data from certain credit and debit cards that were used from September 20, 2013 to August 7, 2014 at Cape May - Lewes Ferry's terminals and vessels may be at risk. The credit and debit card data potentially at risk includes the card number, the cardholder's name and/or the card's expiration date. We have not determined that any *specific* cardholder's credit or debit card data was stolen by the intruder.

"We take the security of our customers' personal information very seriously and work extremely hard to protect their credit and debit card data," said Heath Gehrke, Director of Ferry Operations. "Despite any company's best efforts, intrusions can occur. With the help of professional experts, we want to understand the nature and scope of this incident so we can learn from it." The Authority is also working with these experts to enhance the security of its credit and debit card processing systems at the Cape May-Lewes Ferry's terminals and vessels. Gehrke emphasized that the food, beverage, and retail locations at the Cape May - Lewes's terminals and vessels have been processing credit and debit card transactions securely since August 8, 2014. Gehrke also stressed that only food, beverage, and retail sales locations were affected by the security compromise. The Cape May - Lewes Ferry reservation system, including on-line bookings and terminal point-of-sale locations, utilized for the purchase of vehicle or passenger tickets was not compromised.

Please visit http://cmlf.com/notification to learn more about this data security event and the identity protection services being provided for potentially affected customers.

The Authority encourages its customers to remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, Cape May-Lewes Ferry customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069,

800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. State Attorneys General may also have advice on preventing identity theft, and instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

We regret any inconvenience this security compromise may have caused our customers. To better assist our customers whose card data may potentially have been affected, Cape May-Lewes Ferry has established a confidential hotline to answer questions. This hotline is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. C.S.T. and can be reached at 1-855-865-4457. Customers can also visit http://cmlf.com/notification for additional information.