



# Cape May – Lewes Ferry PRESS RELEASE

October 24, 2014  
For Immediate Release

**Contact**  
**James E. Salmon**  
**(302) 571-6409**

## Notice of Data Security Event

(New Castle, DE) - 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](http://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

-more-

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](http://www.equifax.com); Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, [www.experian.com](http://www.experian.com); or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, [www.transunion.com](http://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/](http://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](http://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](http://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.

###