McDonald Hopkins
A business advisory and advocacy law firm®

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

March 31, 2017

VIA E-MAIL: consumer@iowa.gov

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

Re: Lincoln Savings Bank – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Lincoln Savings Bank ("Lincoln"). I write to provide notification concerning an incident that may affect the security of personal information of two thousand, one hundred thirty-three (2,133) Iowa residents. Lincoln's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Lincoln does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On or about February 2, 2017, Lincoln learned that one of its then-current employees had sent, without having a job-related reason to do so, an electronic document to his personal e-mail account on January 4, 2017 which contained information regarding certain Lincoln customers' accounts. Lincoln also was made aware that some former Lincoln employees may have sent and/or received certain Lincoln customers' sensitive account information through their personal e-mail accounts. These employees had legitimate access to customers' account information as a result of their employment with Lincoln, but exceeded that authorization by inappropriately accessing this information. Lincoln's discovery of these unauthorized actions has led to the conclusion that these rogue employees misappropriated the customer information to try to gain a strategic advantage for alternative employment opportunities with a competing bank.

Upon learning of the issue, Lincoln promptly launched a full investigation, including reporting the incident to the appropriate regulatory agencies, terminating the employee who was still working for Lincoln in accordance with the company's policies and procedures, and sending cease and desist letters to the individuals involved and their new employer. Lincoln also has devoted considerable time and effort to determine exactly what information was sent and/or received by the individuals in question and, as such, whose information may have been compromised.

On March 15, 2017, Lincoln's investigation and related comprehensive document review concluded and determined that the personal information improperly accessed and/or retained by the

former Lincoln employees included residents' full names, home addresses, dates of birth and Social Security numbers. In addition, the bank account information and/or credit/debit card numbers belonging to twenty-four (24) residents were involved in this incident.

To date, Lincoln is not aware of any reports of identity fraud or financial harm to its customers as a direct result of this incident. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps Lincoln is taking to safeguard the residents against identity fraud. Lincoln will provide the Iowa residents with written notice of this incident commencing on March 31, 2017, in substantially the same form as the letter attached hereto. Lincoln will advise the residents to remain vigilant in reviewing financial and credit card account statements for fraudulent or irregular activity on a regular basis. Lincoln will advise those residents whose bank information was involved in this incident to contact their financial institution to determine if their bank account should be changed, and also will advise the residents whose credit/debit card numbers were involved to contact their bank or card issuer to determine whether a new card should be issued to them. Lincoln will offer the residents a complimentary membership with a credit monitoring and identity theft protection service, and also will provide dedicated call center support to answer questions. Lincoln will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Lincoln is committed to maintaining the privacy of its customers' information, and continually evaluates and modifies it practices to enhance the security and privacy of customers' information. In light of this incident, Lincoln is taking proactive steps to prevent recurrence of this situation, including conducting ongoing training and counseling of its workforce regarding customer privacy matters and implementing procedures to check for outgoing emails containing sensitive and personal information.

In addition, Lincoln has been engaged in ongoing discussions with the former employees involved and has sought their assurances that its customers' personal information was not copied, downloaded, printed, or shared with any other third parties. Lincoln also has notified the appropriate regulatory authorities so that they can coordinate with other banks to monitor for fraudulent activity on the customer information that was obtained by the unauthorized parties in question.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

DAP/sdg
Encl.

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

March 31, 2017

Dear [redacted],

The privacy and security of your personal information is of utmost importance to Lincoln Savings Bank ("Lincoln") and we take significant measures to protect it. I am writing to you with important information about a recent incident which may involve the security of some of your personal information we maintain. We want to provide you with information regarding the incident, explain the services we are making available to help safeguard you against identity fraud, and provide steps you can take to help further protect your information.

On or about February 2, 2017, we learned that a Lincoln employee sent, without having a job-related reason to do so, an electronic document to his personal e-mail account on January 4, 2017 which contained information regarding certain Lincoln customers' accounts. We also were made aware that some former Lincoln employees may have sent and/or received certain Lincoln customers' sensitive account information through their personal e-mail accounts. These employees had legitimate access to customers' account information as a result of their employment with Lincoln, but exceeded that authorization by inappropriately accessing this information. Our discovery of these unauthorized actions has led to the conclusion that these rogue employees misappropriated the customer information to try to gain a strategic advantage for alternative employment opportunities with a competing bank.

We take this situation very seriously, and are taking all appropriate steps to notify you so that you may take action along with our efforts to minimize any potential misuse of your information. Upon learning of the issue, we promptly launched a full investigation, including reporting the incident to the appropriate regulatory agencies, terminating the employee who was still working for us in accordance with our policies and procedures, and sending cease and desist letters to the individuals involved and their new employer. We also have devoted considerable time and effort to determine exactly what information was sent and/or received by the individuals in question and, as such, whose information may have been compromised.

On March 15, 2017, our investigation and related comprehensive document review concluded and we determined that the personal information improperly accessed and/or retained by the former Lincoln employees included your full name, home address, date of birth, Social Security number, bank account information and credit/debit card number. We have no evidence to suggest that any other personal information of yours was accessed and/or retained.

Because we value our relationship with you, we wanted to make you aware of this incident and let you know that we are engaged in ongoing discussions with the former Lincoln employees involved and have sought their assurances that your personal information was not copied, downloaded, printed, or shared with any other third parties.

To date, we are not aware of any reports of identity fraud or financial harm to you as a direct result of this incident. Out of an abundance of caution, however, we want to take extra precautions to protect you from potential misuse of your information and are providing you with one year of free credit monitoring and identity theft protection services through Experian's ProtectMyID® Alert. Enclosed in this letter you will find information on how to enroll in a 12-month membership that we are providing at no cost to you. This robust product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Also enclosed, you will find other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files and obtaining a free credit report. Since your bank account information was involved, we recommend you contact your financial institution to determine if your bank account should be changed. Additionally, you should always remain vigilant in reviewing your credit card and financial account statements for fraudulent or irregular activity on a regular basis.

You should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

On behalf of Lincoln, please accept our sincerest apologies that this incident occurred. We value you as a customer and your trust and security are our top priorities. We are committed to maintaining the privacy of our customers' information, and we continually evaluate and modify our practices to enhance the security and privacy of our customers' information, including the ongoing training and counseling of our workforce regarding customer privacy matters, and implementing procedures to check for outgoing emails containing sensitive and personal information. In light of this incident, Lincoln is taking proactive steps to prevent recurrence of this situation.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time.

Sincerely,

[redacted]

Emily J. Girsch, CPA, MBA
Executive Vice President/Chief Financial Officer
Lincoln Savings Bank

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Lincoln Savings Bank. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted].
2. VISIT the ProtectMyID Web Site to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] and provide Engagement # [redacted].

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-888-766-0008

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111
1-800-349-9960 (NY residents only)

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you live in ***Iowa***, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General
Consumer Protection Division
1305 East Walnut Street
Des Moines, IA 50319
(515) 281-5164
1-888-777-4590
Fax: (515) 281-6771
www.iowaattorneygeneral.gov

If you live in ***Maryland***, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

If you live in ***North Carolina***, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Instances of known or suspected identity theft should also be reported to law enforcement.

6. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.