Texas Department of
Savings and Mortgage Lending

From: Caroline Jones, Commissioner
To: State Savings Bank Presidents and Chief Executive Officers

---

May 16, 2017

SUBJECT: WannaCry Ransomware; Response Required by Close of Business May 17, 2017

As you know from news reports, a global ransomware campaign is affecting over 100,000 computers in more than 155 countries. The ransomware exploits a vulnerability in Microsoft Windows. The issue primarily relates to "computer hygiene," that is, keeping your computers up-to-date and patched. Specific information about patching for this exploit is on the US-CERT website (see link below under #3). The FFIEC has released two joint statements in the past related to patch management and protecting your bank against this and similar threats. I encourage you to review those:

•FFIEC Joint Statement on Destructive Malware:
https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

•FFIEC Joint Statement on Cyber Attacks Involving Extortion:
https://www.ffiec.gov/press/PDF/FFIEC_Joint_Statement_Cyber_Attacks_Involving_Extortion_-_Interactive_Ve%20%20%20.pdf

In addition to alerting you about this issue, we are determining the status of the Texas thrift industry and its readiness in this situation. Due to the quick-spreading nature of the ransomware, please let us know the following information by **close of business, Wednesday, May 17th.** If your answers are not sensitive, please reply to Stephany Trotti at strotti@sml.texas.gov. If your answers are sensitive or if you would like to discuss your response, please contact Stephany Trotti at 512-738-2603.

1) Name of Bank, City, approximate total assets

2) Have any of the bank's systems been infected with the WannaCry ransomware (or other variants)?

3) Has the bank updated its systems and applied the Microsoft patch for the MS-17-010 SMB vulnerability dated March 14, 2017? If not, see the information on the US-CERT website https://www.us-cert.gov/ncas/alerts/TA17-132A.

4) If the bank has been impacted by the ransomware, what have you done to address the issue? If you have not contacted law enforcement, we strongly encourage you to contact a local FBI or US Secret Service field office to report an intrusion and request assistance.

Thank you,

Caroline Jones
Commissioner