Keep Your Personal Data Secure Online

At Hawaii National Bank, the security of your information is our top priority. We take proactive measures to stay ahead of security risks and prevent your personal data from being compromised. When using our convenient Online and Mobile Banking tools, we encourage you to follow several important guidelines recommended by the Federal Financial Institutions Examination Council (FFIEC) to keep your information secure:

1. Review your financial statements and monitor transactions on a weekly basis. Our Online, Mobile and ATM Banking tools allow you to see up-to-date transaction information.

2. Lock your electronic devices when you leave them unattended, and always log off from Online or Mobile Banking services when you complete your session.

3. Never use publicly available information to create your password. This includes common names and phrases, birthdates and social security numbers.

4. Change your passwords every few weeks to reduce the risk of a compromised account, and avoid using password managers, which can make it easy to forget passwords over time.

5. Keep your passwords and pin numbers confidential.

6. Never click on links or applications in e-mail, as those are common ways viruses, malware and malicious software are installed. If you are uncertain about any communications you receive from Hawaii National Bank, please call us at (808) 528-7711.

7. When banking online, always use a secure connection, noted by https:// in front of our web address (https://www.HawaiiNational.BANK). This indicates that the data being transmitted between your browser and our systems is securely encrypted.

8. Install anti-virus and anti-malware software on your electronic devices, and update it regularly. All mobile software should be downloaded from the Android Market or the Apple App Store and never from a third-party site. Read the application permissions carefully.

9. Install software capable of remotely wiping your electronic devices if they are stolen or lost, and notify your mobile carrier as soon as possible if an incident occurs.

10. Do not "jailbreak" your iPhone or "root" your Android. This may make them susceptible to malicious software.

11. Turn off wireless device services such as Wi-Fi, Bluetooth and GPS when they are not being used.

12. Avoid using unsecured public wireless connections unless you have virtual private network (VPN) software installed.

13. Statistics show that users of social networking sites experience a higher incidence of fraud. Use privacy settings to control who is able to access your personal information.

14. Hawaii National Bank offers alerts to notify you of activity on your accounts. You can set up alerts when you login to your Online Banking account.

15. Sign up for electronic banking statements and use our convenient Online Bill Pay features whenever possible. The fewer paper documents with your account information on them, the better.