



State of Washington

DEPARTMENT OF FINANCIAL INSTITUTIONS  
DIVISION OF BANKS

P.O. Box 41200 • Olympia, Washington 98504-1200

Telephone (360) 902-8704 • TDD (360) 664-8126 • FAX (360) 586-5068 • <http://www.dfi.wa.gov/banks>

**TO:** Chief Executive Officers and IT Managers of Washington State Regulated Institutions  
**RE:** Immediate Action Needed to Address the “Heartbleed” Vulnerability  
**DATE:** April 11, 2014

The Washington State Department of Financial Institutions – Division of Banks (“Division”) is aware that a major breakdown in Internet security, called the Heartbleed internet bug (“Heartbleed bug”), has the potential to compromise millions of passwords, credit card numbers, and other personal information.

The Heartbleed bug appears to have been introduced by a programming mistake in a version of OpenSSL. The ramifications of this breach are unknown at this time, but it has been reported that customer information may have already been compromised by hackers. The Heartbleed bug may have gone undetected for more than two years.

What should my institution do?

- If your institution’s website or any outsourced third-party vendors’ website uses OpenSSL, verify that the patch for the Heartbleed bug has been implemented.
  - Remember to verify vendors that customers access outside of your bank’s website, such as remote deposit capture and certain cash management applications.
  - To quickly see if your institution may be affected, go to this website and enter your website address: <https://lastpass.com/heartbleed/>.
- If your website or your third-party vendor sites are affected, ensure the appropriate fix is implemented immediately.
- Consider communicating to your customers as to whether the bug has been fixed.
- Consider advising customers to change their passwords after you have determined that the site is safe.
- Consider placing a notice on your website informing customers that the site is safe and/or has been updated.
- Review your institution’s internal policies and procedures to ensure they adequately address similar situations.

What is DFI doing?

- The Division is verifying that all regulated institutions have implemented the patch to the Heartbleed bug.
- If your institution appears vulnerable, a representative from the Division will be contacting you to ensure that the problem has been fixed.

The FDIC has also issued the following Financial Institution Letter (FIL-16-2014) discussing the Federal Financial Institutions Examination Council Alert: *OpenSSL “Heartbleed” Vulnerability Alert*

<http://www.fdic.gov/news/news/financial/2014/fil14016.html>