CONSUMER ALERT

Wisconsin Department of Agriculture, Trade & Consumer Protection datcp.wisconsin.gov

"Ransomware" Scam Tying Up Personal Computers

Release Date: **September 12, 2012** **Contact:** **Jerad Albracht, 608-224-5007**
Jim Dick, Communications Director, 608-224-5020

MADISON – If your computer locks up and a screen appears telling you that you owe a fine for accessing illegal material on the internet, you are the victim of Reveton "ransomware."

"The FBI has issued a warning about ransomware, and now we're hearing from Wisconsin consumers who are victims," says Sandy Chalmers, Administrator of Trade and Consumer Protection. "Use caution when online, and don't pay money to unlock your computer."

Unlike a traditional virus which infects computers when the user opens a file or attachment, Reveton infects a computer when the user clicks on a compromised website.

Here is how the scam works:

- A computer is infected with Reveton and the computer immediately locks up.
- The computer displays a fake message from the FBI or the U.S. Department of Justice. This ransom screen warns the user that they have violated federal laws and that the computer's IP address was identified as having visited illegal content on the web.
- The user is prompted to pay a fee (typically $100-$200) using a prepaid money card service in order to have control of their systems returned. The user is directed to submit the code from their money card via an input box on the ransom screen.
- After paying the fee, the screen will be removed. But the malware may continue to operate on the compromised computer and can be used to commit online banking and credit card fraud.

If your computer is locked down by the virus, the federal Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, recommends that you:

- Do not pay any money or provide any personal information.
- Contact a computer professional to remove Reveton and Citadel (a host program) from your computer.
- Be aware that even if you are able to unfreeze your computer on your own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords and credit card numbers through embedded keystroke logging programs.
- File a complaint and look for updates about the Reveton virus on the IC3 website: www.ic3.gov.

For additional consumer information, visit the Wisconsin Bureau of Consumer Protection's website at datcp.wisconsin.gov. You can also contact us via e-mail at datcphotline@wisconsin.gov or by phone at 1-800-422-7128.

Connect with us at facebook.com/wiconsumer.

###