FOR Immediate RELEASE

Princeton, MO – August 28, 2017

GRM Networks strongly urges all customers to beware of a new, more malicious, variant of the original malware called Locky Ransomware. It is spread by spam email that comes with a .zip attachment, containing a .js or .vsb file inside.

If your system is infected with Locky Ransomware, your data will be encrypted and there is no known decrypt currently available. Additionally, it is possible for this malware to spread through networks, so it is critical that all team members receive proper training on how to avoid this issue.

Please follow these important tips to reduce the likelihood that your system is infected with Locky Ransomware:

- If you receive an email attachment of any kind, treat it with caution especially if it's a .zip file.
- Before opening any attachment, ensure that you know the sender and that you were expecting an attachment from them.
- Double-check email headers to ensure they are legitimate.
- Remember: "When in doubt, throw it out!"

If you have questions or concerns about your GRM Networks Internet service, please call technical support at 1-800-721-2577 or go to our website www.grm.net for alert notifications.

About GRM Networks®

GRM Networks® is a member owned cooperative that provides communication services to customers located within a 4,500 square mile radius that covers 44 exchanges in northern Missouri and southern Iowa. GRM Networks® is dedicated to delivering reliable, advanced communications technology while providing an exceptional customer experience. GRM Networks® is committed to promoting and investing in its local communities. LTC Networks® & SCC Networks® are subsidiaries of GRM Networks®. For more information about GRM Networks®, visit www.grm.net.