BLANK ROME LLP
COUNSELORS AT LAW

Phone: *(215) 569-5352*
Fax: *(215) 832-5352*
Email: *Lee-M@BlankRome.com*

December 20, 2013

Karl Steinborn
1704 Quail Valley East
Columbia, SC 29212-1531

Dear Mr. Steinborn:

This law firm represents Rich Gorman and his related companies. Mr. Gorman has recently received a number of extremely disturbing email communications which threaten harm to Mr. Gorman, his businesses, and his customers, if he does not make a payment of several thousand hundred dollars worth of Bitcoins as directed in the emails. The threatening tone of the emails has been escalating in recent days. In addition, derogatory and/or defamatory information about Mr. Gorman has been recently posted on numerous websites.

Our preliminary investigation into this matter suggests to us that you have a connection with www.performoutsider.com, a web site which appears to be related to these threatening emails and defamatory postings. We therefore hereby demand that you immediately cease and desist from posting, or causing to be posted, any derogatory or defamatory information about Mr. Gorman, or any of his affiliates, employees, business associates, and/or customers.

Please be advised that Mr. Gorman is presently evaluating his legal options and intends to take appropriate action to protect his legal rights, including the possible referral of the matter to appropriate legal authorities.

Finally, please regard this letter as requesting that you preserve documents, tangible things, and electronically stored information potentially relevant to the issues referenced in this letter. You should anticipate that much of the information relevant to this matter is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones). Electronically stored information (hereinafter "ESI") should be afforded the broadest possible meaning and includes, by way of example and not as an exclusive list, potentially relevant information electronically, magnetically, optically, or otherwise stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- E-Mail Server Stores (e.g., Lotus Domino .NSF or Microsoft Exchange .EDB)
- Word processed documents (e.g., Word or WordPerfect files and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, blog entries);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and
- Backup and Archival Files (e.g., Veritas, Zip, .GHO)

ESI resides not only in areas of electronic, magnetic, and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both sources of ESI, even if you do not anticipate producing such ESI.

Preservation Requires Immediate Intervention

If you have not already done so, you should act immediately to preserve potentially relevant ESI concerning this matter. Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must intervene to prevent loss due to routine operations or malfeasance and employ proper techniques and protocols to preserve ESI. Booting a drive, examining its contents, or running any application may irretrievably alter the evidence it contains and constitute unlawful spoliation of evidence. As such, preservation of potentially relevant information requires your immediate attention and action. Federal and state laws require that you retain certain documents. This preservation letter includes those documents to be retained under state and federal law as well as documents and date described herein.

Nothing in this request for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things, and other potentially relevant evidence. Moreover, this request to preserve information for this litigation is both retroactive and prospective in application, which means that it extends to all documents, tangible things, and

electronically stored information that currently exist relating to this lawsuit, as well as all documents, tangible things, and electronically stored information that are created in the future during the course of this litigation.

Suspension of Routine Destruction
You are requested to immediately initiate a litigation hold for potentially relevant ESI, documents, and tangible things and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further requested to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity, or other criteria;
- Using data or media wiping, disposal, erasure, or encryption utilities or devices;
- Overwriting, erasing, destroying, or discarding backup media;
- Re-assigning, re-imaging, or disposing of systems, servers, devices, or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server, packet, or local instant messaging logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion and Act to Prevent Spoliation
You should take affirmative steps to prevent anyone with access to your data, systems, and archives from seeking to modify, destroy, or hide ESI on network or local hard drives and on other media or devices (such as by deleting or overwriting files; using data shredding and overwriting applications; defragmentation, re-imaging, damaging, or replacing media; encryption; or compression).

Preservation of Backup Tapes
You are requested to preserve complete backup tape sets (including differentials and incrementals) containing ESI related to this matter.

You should anticipate that ESI will be sought in the form or forms in which it is ordinarily maintained (i.e., native form). The forensically sound image described above will preserve ESI in such native form. You should not employ methods to preserve ESI that remove or degrade the ability to search the ESI by electronic means or that make it difficult or burdensome to access or use the information. You should additionally refrain from actions that shift ESI from reasonably

accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata
You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files, but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields. Metadata may be overwritten or corrupted by careless handling or improper preservation, including by moving, copying or examining the contents of files.

Servers
With respect to servers used to manage e-mail (e.g., Microsoft Exchange, Lotus Domino) and network storage (often called a "network share"), the complete contents of each user's network share and e-mail account should be preserved if that user has potential relevance to this matter. There are several ways to preserve the contents of a server. If you are uncertain whether the preservation method you plan to employ is one that we will accept as sufficient, please immediately contact the undersigned.

Home Systems, Laptops, Online Accounts and Other ESI Venues
Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems or devices may contain potentially relevant data. To the extent that you have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, memory stick, CDR/DVD-R disks, and the user's PDA, smart phone, voice mailbox, or other forms of ESI storage.). Similarly, if you used online or browser-based e-mail accounts or services (such as Gmail, AOL, or Yahoo Mail) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted, and Archived Message folders) should be preserved.

Ancillary Preservation
You should preserve documents and other tangible items that may be required to access, interpret, or search potentially relevant ESI, including but not limited to logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, and user ID and password rosters. You should preserve passwords, keys, and other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals, and license keys for applications required to access the ESI. You should preserve cabling, drivers, and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives, and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate
As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys, and Third Parties
Your preservation obligation extends beyond ESI in your care, possession, or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you should notify any current or former agent, attorney, employee, custodian, and contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you should take reasonable steps to secure their compliance.

Sincerely yours,

MATTHEW D. LEE