



June 2, 2015

Laura A. Brevetti
General Counsel and Secretary
WWE, Inc.
1241 East Main Street
Stamford, CT 06902

RE: Notice of Representation of Former WWE Wrestler Ivan Koloff

Dear Attorney Brevetti:

Please be advised that the undersigned have been retained by Ivan Koloff, a former WWE wrestler whose stage name was “Russian Bear” and who was allegedly injured as a result of WWE’s negligent and fraudulent conduct. In light of the possible litigation involving this matter, we would like to remind you and the WWE, its employees, agents, and assigns (“you”) to refrain from both communicating directly with our client and from allowing any spoliation of evidence relevant or pertaining to Mr. Koloff’s claims.

The duty to preserve relevant data arises when you have reasonable anticipation of litigation. As such, we presume that all parties will take the necessary steps to preserve data in all forms, both physical and electronic. Such particular data relevant to this matter include personnel records, contracts, medical records during the years Mr. Koloff was contracted with WWE, royalties’ accountings, licenses, deals, toys, action figures, video games, DVDs, streaming videos on the WWE Network, any recordings of performances, including training and “house” performances, and any communications between Mr. Koloff and the WWE, as well as any communications between WWE and their employees, agents, or assigns involving or discussing Mr. Koloff. Of particular importance, but not limited to, are any communications regarding wrestler safety, training, medical attention, or injury and Mr. Koloff, as well as any communications regarding Mr. Koloff’s employment with the WWE.

Electronically stored information should be afforded the broadest possible definition and includes by way of example the following list of potentially relevant information electronically, magnetically, or optically stored as:

- Digital communications such as email, voice mail, text messaging, instant messaging, and social media platforms, including but not limited to Facebook, Twitter, SnapChat, Confide, Instagram, or Vine;
- Word-processing documents such as Microsoft Word and drafts of the same;
- Spreadsheets and tables such as Microsoft Excel or Lotus 123 worksheets;
- Accounting Application Data such as QuickBooks, Money, and Peachtree data files;

- Image and Facsimile Files such as .pdf, .tiff, .jpg, .jpeg, and .gif files;
- Sound Recordings such as .wav, .mp3, and .mp4 files;
- Videos and Animations such as .avi and .mov files;
- Databases such as Microsoft Access, Oracle, SQL Server data, and SAP;
- Contact and Relationship Management Data such as Microsoft Outlook;
- Calendar and Diary Application Data such as Microsoft Outlook PST, Yahoo, Google Calendar, and blog tools;
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design / Drawing Files; and
- Back Up and Archival Files such as .zip, .gho, and .7z;

Although this list is not exhaustive, you are obliged to take affirmative steps to prevent anyone with access to your data, systems, and archives from seeking to modify, destroy, or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography, or the like). With respect to workstation and laptop hard drives, one way to protect existing data on the hard drives is the creation and authentication of a forensically-qualified image of all sectors of the drive. Such a forensically-qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up or “Ghosting” of a hard drive are not forensically-qualified procedures because they capture only active data files and fail to preserve forensically-significant data that may exist in such areas as unallocated space, slack spaces and the swap file.

For the hard drives and other digital storage devices of every person involved with the hiring, training, coaching, match discussion, match preparation, medical attention, medical diagnosing, medical discussions, injury discussion, or employment of Mr. Koloff, and of each person acting in the capacity of CEO, COO, CFO, hiring manager, event organizer, performance writer, booking agent, trainer, coach, other wrestlers, or on-site and off-site medical personnel with any data or information relating to this matter, as well as each other person likely to have information pertaining to the instant matter on their computer hard drive(s) or other electronic storage media, demand is made that you immediately obtain, authenticate and preserve forensically-qualified images of the hard drives and other storage media in (or used in conjunction with) any computer system (including portable and home computers) used by that person during the period from Mr. Koloff's performances until today, as well as recording and preserving the system time and date of each such computer.

You should anticipate that your employees, officers, or other may seek to hide, destroy, or alter relevant data both electronic and physical, and you must act to prevent or guard against such actions. Users may seek to delete or destroy information they regard as personal, confidential, or embarrassing and, in so doing, may also delete or destroy potentially relevant data. Even personally owned laptops, desktops, tablets, and cell phones with relevant communications and / or data must be preserved.

Please take the time to inform and advise *every* custodian of discoverable data relevant to this pending matter to ensure their compliance with the requirements for discovery and the

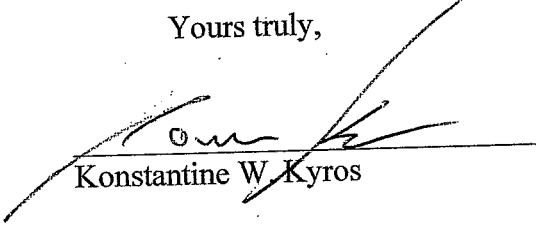
prevention of the spoliation of evidence. This includes refraining from overwriting deleted data on magnetic media, encrypting data and losing the encryption key, and/or physically damaging the media. This might also include halting server protocols and preventing custodians of discoverable data from taking, among other actions, the following actions:

- 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 back-up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting the wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and
- Executing drive or file defragmentation or compression programs.

Such custodians are also advised that not only electronic data must be preserved. Cell phones, costumes, letters, facsimiles, and all documents in paper form, along with all physical items in the image and likeness of Mr. Koloff should be preserved and have a litigation hold established on them.

Please confirm by June 22 that you have taken the necessary steps outlined in this letter to preserve data and documents potentially relevant to this matter. If you have not undertaken the steps outlined in this letter, or have taken other actions, please describe in your response what you have done to preserve the potentially relevant evidence. Please also forward us copies of any booking contracts or agreements that may govern these claims.

Yours truly,



Konstantine W. Kyros

Telephone: (800) 934-2921
kon@kyroslaw.com

CC: Robert K. Shelquist
Charles J. LaDuca
Erica C. Mirabella
Harris L. Pogust