LAW OFFICES OF ABE GEORGE, P.C.

44 Wall Street, 2nd Floor
New York, New York 10005
(P) 212-498-9803 (F) 646-558-7533
Email: abe@abegeorge.lawyer

June 27, 2017

VIA FIRST CLASS & ELECTRONIC MAIL DELIVERY ONLY

Kellogg Company
One Kellogg Square
Battle Creek, Michigan 49017
Attention: Messrs. John A. Bryant, Brian S. Rice, Fareed A. Khan, David Biller, Ted Engle & James M. Yany, Gary H. Pilnick, Esq., General Counsel, Gordon Paulson, Esq., Corporate Counsel, Erik W. Chalut, Esq., Corporate Counsel, Jeffrey J. Canfield, Esq., Corporate Counsel, James K. Lewis, Esq., Corporate Counsel, & Daniel A. O'Connor, Esq., Corporate Counsel
Email: john.bryant@kellogg.com
Email: brian.rice@kellogg.com
Email: fareed.khan@kellogg.com
Email: david.biller@kellogg.com
Email: ted.engle@kellogg.com
Email: james.yany@kellogg.com
Email: gary.pilnick@kellogg.com
Email: gordon.paulson@kellogg.com
Email: erik.chalut@kellogg.com
Email: jeffrey.canfield@kellogg.com
Email: jim.lewis@kellogg.com
Email: daniel.oconnor@kellogg.com

W. M. Brown Group, Inc.
219 Lafayette Drive
Syosset, New York, 11791-3939
Attention: Messrs. Warren M. Brown & Michael Ambrosia
Email: chartmann@wmbrowngroup.com
Email: mambrosia@wmbrowngroup.com

Two Locks Inc. d/b/a Premier Snacks
169 Commack Road, Suite 377
Commack, New York, 11725
Attention: Mr. Marc Ceruto
Email: marc@premierdsd.com

Re: NOTICE OF DEMAND for Preservation of Documents and Electronically Stored Information in Anticipation of Litigation

June 27, 2017
Kellogg Company
W. M. Brown Group, Inc.
Two Locks Inc. d/b/a Premier Snacks

Dear Gentlemen:

Reference is made to this law firm's letter dated June 13, 2017 ("June 13, 2017 Letter"), a copy of which I attach for your reference. As you are aware, this firm has officially been retained and represents over fifteen (15) distributors (each individually, a "Client", and collectively, this firm's "Clients") that hold exclusive rights to deliver Kellogg Company's ("Kellogg") snack products. Mr. O'Connor from Kellogg has verbally acknowledged receipt of the June 13, 2017 Letter requesting additional time to respond while representatives from both W. M. Brown Group Inc. and Two Locks Inc. have failed to contact the undersigned at all. Nevertheless, as part of this representation and in anticipation of the filing of a class action lawsuit relating to my Clients' claims against Kellogg *et al.* as further set forth in the June 13, 2017 Letter, I am writing to remind you of your legal duties pursuant to the requirements of both New York state law and Rules 26 and 37 of the Federal Rules of Civil Procedure to identify and preserve all relevant materials that may relate to this matter, directly or indirectly, to the underlying dispute between or among the parties.

Therefore, this letter shall serve to hereby demand that you preserve all documents, tangible things and electronically stored information potentially relevant to the issues in this cause. As used in this demand letter, "you" and "your" refers to Kellogg Company, W. M. Brown Group, Inc. and Two Locks Inc. d/b/a Premier Snacks, together with respective predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

You should anticipate that much of the information subject to disclosure or responsive to discovery in 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, servers and cell phones).

Electronically stored information (hereinafter referred to as "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as: (i) Digital communications (e.g., e-mail, voice mail, instant messaging); (ii) Word processed documents (e.g., Word or WordPerfect documents and drafts); (iii) Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets); (iv) Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files); (v) Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images); (vi) Sound Recordings (e.g., .WAV and .MP3 files); (v) Video and Animation (e.g., .AVI and .MOV files); (vi) Databases (e.g., Access, Oracle, SQL Server data, SAP); (vii) Contact and Relationship Management Data (e.g., Outlook, ACT!); (viii) Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools); (ix) Online Access Data (e.g., Temporary Internet Files, History, Cookies); (x) Presentations (e.g., PowerPoint, Corel Presentations) (xi) Network Access

and Server Activity Logs; (xii) Project Management Application Data; (xiii) Computer Aided Design/Drawing Files; and (xiv) Back Up and Archival Files (e.g., 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 these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/06), a party must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible. For good cause shown, please note that a court may then order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive my Clients of their right to secure the evidence or a court of its right to adjudicate the issue

Preservation Requires Immediate Intervention. You must act immediately to preserve potentially relevant ESI including, without limitation, information with the earlier of a 'Created or Last Modified' date on or after June 23, 1994 through the date of this demand and concerning:

1. The events and causes of action described in the June 13, 2017 Letter;
2. ESI you may use to support claims or defenses in this case; and
3. All communications between or among any of the parties at issue, or their principals, agents, or employees.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Please be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI. Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve document, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction. You are directed 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 directed 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: (i) Purging the contents of e-mail repositories by age, capacity or other criteria; (ii) Using data or media wiping, disposal, erasure or encryption utilities or devices; (iii) Overwriting, erasing, destroying or discarding back up media; (iv) Re-assigning, re-imaging or disposing of systems, servers, devices or media; (v) Running antivirus or other programs effecting wholesale metadata alteration; (vi) Releasing or purging online storage repositories; (vii) Using metadata stripper utilities; (viii) Disabling server or IM logging; and (ix) Executing drive or file defragmentation or compression programs.

If you need to continue to access any ESI that is subject to the preservation obligations, please contact me first so that we can consider the best way to proceed. This is important because if you open, move, copy or archive relevant ESI, or forward or compact relevant emails, etc., these actions may automatically alter metadata that may be important, or lead to the accidental deletion of ESI.

Guard Against Deletion. Considering the recent press articles regarding the matter at issue, you should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that 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 ESI. This concern is not one unique to you or your employees and officers. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Preservation by Imaging. You should 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 local hard drives, one way to protect existing data on local hard drives is by 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 of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

With respect to the hard drives and storage devices of each of the persons named below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home

computers) used by the following individuals during the period from June 23, 1994 to the present day, as well as recording and preserving the system time and date of each such computer:

1. James M. Yany, Executive at Kellogg Company;
2. Ted Engle, Sales Director at Kellogg Company;
3. Jeffrey Bunzel, Executive at Kellogg Company;
4. Omar Zlam, Senior Manager at Kellogg Company;
5. Cheri O'Neill, Executive at Kellogg Company;
6. David Biller, Account Executive at Kellogg Company, former manager of Two Locks Inc. d/b/a Premier Snacks;
7. Warren M. Brown, President at W. M. Brown Group, Inc.;
8. Michael Ambrosia, General Manager at W. M. Brown Group, Inc.;
9. Marc Ceruto, President at Two Locks Inc. d/b/a Premier Snacks; and
10. Sydney Ceruto, Vice President at Two Locks Inc. d/b/a Premier Snacks.

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

Preservation in Native Form. You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

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. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. 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.

Servers. With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that we will accept as sufficient, please call me to discuss it.

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 may contain potentially relevant data. To the extent that officers, board members or employees 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, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) 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 must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like. You must preserve any passwords, keys or 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 must preserve any 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. 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

Paper Preservation of ESI is Inadequate. As hard copies do not preserve electronic search-ability 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 must notify any current or former agent, attorneys (such as Jenner & Block LLP), employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging. We suggest that, with respect to James M. Yany, Ted Engle, David Biller, Jeffrey Bunzel, Omar Zlam, Cheri O'Neill, Warren M. Brown, Michael Ambrosia, Marc Ceruto and Sydney Ceruto, removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step.

In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Preservation Protocols. We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

Do Not Delay Preservation. The undersigned is available to discuss reasonable preservation steps; however, you should not defer preservation steps pending such discussions if ESI may be lost or corrupted because of any delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

June 27, 2017
Kellogg Company
W. M. Brown Group, Inc.
Two Locks Inc. d/b/a Premier Snacks

Confirmation of Compliance. Please confirm by July 7, 2017, that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, kindly describe what you have done to preserve potentially relevant evidence. You may reach me at 212-498-9803. Otherwise, please be guided accordingly. Thank you.

Very truly yours,
LAW OFFICES OF ABE GEORGE, P.C.

Abe George, Esq.

Attachments