HARDER MIRELL & ABRAMS LLP

132 S. RODEO DRIVE, FOURTH FLOOR
BEVERLY HILLS, CA 90212
424.203.1600 • WWW.HMAFIRM.COM

January 4, 2018

VIA EMAIL AND OVERNIGHT MAIL
Mr. Steve Rubin, President & Publisher
Henry Holt and Company, Inc.
175 Fifth Avenue
New York, New York 10010
publicity@hholt.com
rights@hholt.com
webmaster@macmillanusa.com

VIA EMAIL
Mr. Michael Wolff
MichaelWolffNYC@gmail.com

Re: Donald J. Trump

Dear Mr. Rubin and Mr. Wolff:

This law firm is litigation counsel for Donald J. Trump ("Mr. Trump"). We are investigating numerous false and/or baseless statements that you have made about Mr. Trump in your upcoming book titled *Fire and Fury: Inside the Trump White House* (the "Book"). A portion of these statements are contained in Mr. Wolff's article published on *New York* magazine's website titled "Donald Trump Didn't Want to Be President," located at http://nymag.com/daily/intelligencer/2018/01 /michael-wolff-fire-and-fury-book-donald-trump.html (the "Article"). Moreover, various excerpts from the Book are published elsewhere.

Your publication of the false/baseless statements about Mr. Trump gives rise to, among other claims, defamation by libel, defamation by libel *per se*, false light invasion of privacy, tortious interference with contractual relations, and inducement of breach of contract. Legal authorities on these and related points are set forth below.

Defamation by Libel and Libel *Per Se*

New York law defines libel as a written statement of fact regarding the plaintiff published by the defendant that is false and causes injury to the plaintiff. *Meloff v. N.Y. Life Ins. Co.*, 240 F.3d 138, 145 (2d Cir. 2001). *See also, Milkovich v. Lorain Journal Co.*. 497 U.S. 1, 111 L.Ed.2d 1,110 S.Ct. 2695 (1990) (U.S. Supreme Court holding that a statement or publication containing provably false factual assertions constitutes defamation); RESTATEMENT (SECOND) OF TORTS, § 559 ("A communication is defamatory if it tends so to harm the reputation of another as to lower

him in the estimation of the community or to deter third persons from associating or dealing with him"); *Dillon v. City of New York*, 261 A.D.2d 34, 37 -38 (1999). Libel *per se* involves a false allegation that a person is engaged in a crime, or that otherwise tends to injure a person in his or her trade, business, or profession. *Geraci v. Probst*, 61 A.D.3d 717, 718, 877 N.Y.S.2d 386, 388 (2009). Libel *per se* is defamatory "on its face" and does not require explanatory matter to be proven; general damages are assumed.

Publication of incomplete and hence misleading information also gives rise to liability for defamation, since the incomplete presentation of facts can imply an actionable false assertion of fact. *See Milkovich v. Lorain Journal Co*., 497 U.S. 1, 19, 110 S. Ct. 2695, 2706, 111 L. Ed. 2d 1,18 (1990) (incomplete facts may imply a false assertion of fact). It also is well established that "defamation by implication stems not from what is literally stated, but what is implied." *White v. Fraternal Order of Police*, 909 F.2d 512, 518 (D.C. Cir. 1990).

Statements in your Article and Book about Mr. Trump (based on excerpts of the Book that have been published thus far) give rise to claims for libel and libel *per se* on the bases described above. Remedies include substantial monetary damages and punitive damages. *Straderv. Ashley*, 61 A.D.3d 1244, 1248, 877 N.Y.S.2d 747, 751 (2009) (affirming jury's award of punitive damages in connection with a defamation claim).

False Light Invasion of Privacy

False light invasion of privacy constitutes a public statement about a person that either is false or places the person in a false light, is highly offensive to a reasonable person, and is made in reckless disregard of whether the information is false or would place the person in a false light. See RESTATEMENT (SECOND) OF TORTS § 652 E (1977); *Machleder v. Diaz*, 801 F.2d 46 (2d. Cir. 1986). The statement need not be defamatory. *Id*. False light invasion of privacy includes embellishment (adding false material to a true story which places the subject in a false light) and distortion (arranging otherwise true information in a way to give a false impression).

Statements in your Article and Book about Mr. Trump (based on excerpts from the Book that have been published thus far) give rise to claims for false light invasion of privacy. Remedies include substantial monetary damages and punitive damages.

Actual Malice

Actual malice (reckless disregard for the truth) can be proven by the fact that the Book admits in the Introduction that it contains untrue statements. Moreover, the Book appears to cite to **no sources** for many of its most damaging statements about Mr. Trump. Also, many of your so-called "sources" have stated publicly that they never spoke to Mr. Wolff and/or never made the statements that are being attributed to them. Other alleged "sources" of statements about Mr. Trump are believed to have no personal knowledge of the facts upon which they are making statements or are known to be unreliable and/or strongly biased against Mr. Trump, or there are

other obvious reasons to question their reliability, accuracy or claims to have knowledge of alleged facts upon which they are purporting to make statements.

Mr. Trump's Demands

Mr. Trump hereby demands that you immediately cease and desist from any further publication, release or dissemination of the Book, the Article, or any excerpts or summaries of either of them, to any person or entity, and that you issue a full and complete retraction and apology to my client as to all statements made about him in the Book and Article that lack competent evidentiary support.

Please also send **immediately** an electronic copy of the full text of the Book, in searchable form, and send via messenger a hard copy of the Book to my office address at the top of this letter, so that we can fully assess all of the statements in the Book.

Inducement of Breach of Mr. Bannon's Written Agreement

Stephen K. Bannon's communications with Mr. Wolff in connection with the Book violated several provisions of Mr. Bannon's written agreement with Donald J. Trump for President, Inc. (the "Agreement"). Mr. Trump, his family members, and their businesses are express third-party beneficiaries of the Agreement. The Agreement contains express provisions preventing Mr. Bannon from:

- Disclosing any confidential information to anyone of or about Mr. Trump, or any of his family members, or any of their businesses, or the campaign;

- Communicating with any members of the print or electronic media about Mr. Trump, or any of his family members, or any of their businesses, or the campaign;

- Disparaging Mr. Trump, or any of his family members, or any of their businesses, or the campaign.

As reflected in the Article and excerpts from the Book, Mr. Bannon has breached each of these provisions by his communications with Mr. Wolff. Now that you are aware of these contractual provisions, and Mr. Bannon's breaches thereof, any publication by you of information provided to you from Mr. Bannon (including quotes from Mr. Bannon about Mr. Trump, or his family members, or their businesses, or the campaign) gives rise to claims of tortious interference with the Agreement, and inducement of Mr. Bannon to breach of the Agreement, among other claims.

Remedies include substantial monetary damages and punitive damages.

In the near future, you should expect to hear from this office in greater detail on all of the foregoing issues.

You are now on notice of the foregoing claims and therefore you are now under a legal duty to affirmatively preserve, and not delete, destroy, hide or misplace, all documents, communications and materials of all types, in both physical and electronic form, that refer to or relate to in any way to the Book and any/all of its contents, the Article and any/all of its contents, Mr. Trump, any/all of his family members, and/all of their businesses, and/or the Donald J. Trump for President campaign.

Preservation Obligations

This demand requires that you affirmatively preserve, and not destroy, delete, hide or misplace, documents and materials of all kinds, including without limitation all electronic mail (email), letters, draft letters, facsimile transmissions, memoranda, draft memoranda, instant messages (IMs), text messages, chats, phone messages, phone logs, calendars, reports, handwritten notes, typewritten notes, charts and spreadsheets, articles, draft articles, photographs, still images, illustrations, video recordings, audio recordings, transcripts of video or audio recordings, among other types of documents and communications. This demand also requires that you affirmatively preserve all servers, backup tapes, hard drives and storage devices in your possession, custody or control and could contain any of the aforementioned documents and/or materials.

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) ("Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("Once a 'litigation hold' is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold'."); *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 620 (D. Colo. 2007) ("To ensure that the expansive discovery permitted by Rule 26(b)(1) does not become a futile exercise, putative litigants have a duty to preserve documents that may be relevant to pending or imminent litigation."); *In re Napster, Inc. Copyright Litigation*, 462 F.Supp.2d 1060, 1067 (N.D. Cal. 2006) (holding that "[a]s soon as a potential claim is identified, a litigant is under a duty to preserve evidence which it knows or reasonably should know is relevant to the action"); *A. Farber & Partners, Inc. v. Garber*, 234 F.R.D. 186, 193 (C.D. Cal. 2006) (same); *Apple Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1136 (N.D. Cal. 2012) (holding that a party has an "obligation to preserve evidence from the moment that litigation is reasonably anticipated.")

Severe sanctions may be imposed for failure to preserve evidence after being notified of a dispute. *Victor Stanley, Inc. v. Creative Pipe, Inc*., 269 F.R.D. 497, 520 (D. Md. 2010) (holding "sanctions may stem from failure to comply with a preservation order."); *Pitney Bowes Gov't Solutions, Inc. v. United States*, 93 Fed. Cl. 327, 336 (2010) ("Spoliation may result in sanctions . . . grounded in contravention of specific discovery or document-preservation orders."); *Pension Committee of the Univ. of Montreal Pension Plan v Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010) (holding that a "breach of the duty to preserve, and

the resulting spoliation of evidence, may result in the imposition of sanctions by a court because the court has the obligation to ensure that the judicial process is not abused."); *Zubulake*, 229 F.R.D. at 430 ("The spoliation of evidence germane 'to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction.'"); *Beers v. General Motors*, 1999 WL 32538 (N.D.N.Y) (ordering **dismissal of case** for spoliation when party's expert lost critical evidence); *Burlington N. & Santa Fe Ry. Co. v. Grant*, 505 F.3d 1013, 1032 (10th Cir. 2007) ("A spoliation sanction is proper where (1) a party has a duty to preserve evidence because it knew, or should have known, that litigation was imminent, and (2) the adverse party was prejudiced by the destruction of the evidence."); *see also Lutalo v. Nat'l R.R. Passenger Corp*., No. 11-CV-00974-REB-KLM, 2013 WL 1294125, at *6 (D. Colo. Mar. 28, 2013) (ordering **evidentiary sanctions and attorneys' fees and costs** on spoliation motion); *Cabinetware, Inc. v. Sullivan*, 1991 WL 327959 (E.D. Cal. 1991); *William T. Thompson Co. v. General Nutrition Corp*., 593 F.Supp. 1443 (C.D. Cal. 1984).

You should anticipate that much of the information requested to be preserved herein is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories, tablets, cell phones and smart phones).

Electronically stored information (hereinafter "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:

- Digital communications (e.g., e-mail, voice mail, instant messages, text messages, chats);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- 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, Yahoo, blog tools);
- 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
- 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 (effective December 1, 2006), you must identify all sources of ESI you decline to produce and demonstrate to the trier of fact why such sources are not reasonably accessible. *See* Fed. R. Civ. P. 26(b)(2)(B). For good cause shown, the trier of fact may then order production of the ESI, even if it finds that it is not reasonably accessible. *Id.* 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 the right of any trier of fact 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 on or after **January 1, 2015 through the present**.

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. **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 documents, tangible things and all 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:

- 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 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.

Guard Against Deletion

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 is 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 with sufficient knowledge or information about this dispute, as well as each other person likely to have information pertaining to the dispute 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 that person during the period from **January 1, 2015 through the present**, as well as recording and preserving the system time and date of each such computer.

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 connection with resolving this dispute.

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. 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 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 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, 3.5" floppy disk drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

Because 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 must notify any current or former agents, attorneys, employees, custodians, contractors and any other third parties 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 any person with sufficient knowledge or information of this dispute, 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. Otherwise, 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 is fair to both sides and acceptable to the trier of fact.

Do Not Delay Preservation

We are available to discuss reasonable preservation steps; however, **you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of 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 all appropriate sanctions.

Confirmation of Compliance

Please confirm to us in writing by no later than **January 5, 2018**, that you will comply with the foregoing instructions and have taken the steps outlined in this document to preserve ESI and tangible documents potentially relevant to this dispute. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Should you have any questions regarding the instructions and requirements hereunder, please do not hesitate to contact me.

This letter is not intended as a full or complete statement of all relevant facts or applicable law, and nothing herein is intended as, nor should it be deemed to constitute, a waiver or relinquishment of any of my client's rights, remedies, claims or causes of action, all of which are hereby expressly reserved.

Very truly yours,

CHARLES J. HARDER Of
HARDER MIRELL & ABRAMS LLP

cc: Donald J. Trump