State of New Jersey
DEPARTMENT OF COMMUNITY AFFAIRS
101 SOUTH BROAD STREET
PO BOX 819
TRENTON, NJ 08625-0819

PHILIP D. MURPHY
Governor

LT. GOVERNOR SHEILA Y. OLIVER
Commissioner

FINAL DECISION

March 27, 2018 Government Records Council Meeting

Marc Mayer
Complainant
v.
Borough of Point Pleasant (Ocean)
Custodian of Record

Complaint No. 2016-186

At the March 27, 2018 public meeting, the Government Records Council ("Council") considered the March 20, 2018 Findings and Recommendations of the Council Staff and all related documentation submitted by the parties. The Council voted unanimously to adopt the entirety of said findings and recommendations. The Council, therefore, finds that:

1. The Custodian has borne her burden of proof that she timely responded to the Complainant's OPRA request based on a warranted and substantiated extension. N.J.S.A. 47:1A-6. Therefore, no "deemed" denial as it related to the extension occurred in the instant matter. N.J.S.A. 47:1A-5(g); N.J.S.A. 47:1A-5(i).

2. The requested records in connection with "complaints and concerns" raised about Officer Kavanagh are exempt from disclosure as "personnel records." N.J.S.A. 47:1A-10; Merino v. Borough of Ho-Ho-Kus, GRC Complaint No. 2003-110 (March 2004). See also Wares v. Twp. of West Milford (Passaic), GRC Complaint No. 2014-274 (May 2015). Thus, the Custodian lawfully denied access to item No. 6 of the Complainant's OPRA request. N.J.S.A. 47:1A-6.

This is the final administrative determination in this matter. Any further review should be pursued in the Appellate Division of the Superior Court of New Jersey within forty-five (45) days. Information about the appeals process can be obtained from the Appellate Division Clerk's Office, Hughes Justice Complex, 25 W. Market St., PO Box 006, Trenton, NJ 08625-0006. Proper service of submissions pursuant to any appeal is to be made to the Council in care of the Executive Director at the State of New Jersey Government Records Council, 101 South Broad Street, PO Box 819, Trenton, NJ 08625-0819.

Final Decision Rendered by the
Government Records Council
On The 27th Day of March, 2018

Robin Berg Tabakin, Esq., Chair
Government Records Council

I attest the foregoing is a true and accurate record of the Government Records Council.

Steven Ritardi, Esq., Secretary
Government Records Council

Decision Distribution Date: March 29, 2018

STATE OF NEW JERSEY
GOVERNMENT RECORDS COUNCIL

Findings and Recommendations of the Council Staff
March 27, 2018 Council Meeting

Marc Mayer[1] **GRC Complaint No. 2016-186**
Complainant

v.

Borough of Point Pleasant (Ocean)[2]
Custodial Agency

Records Relevant to Complaint: See Exhibit A.

Custodian of Record: Antoinette Jones
Request Received by Custodian: June 24, 2016
Response Made by Custodian: June 28, 2016
GRC Complaint Received: July 1, 2016

Background[3]

Request and Response:

On June 24, 2016, the Complainant submitted an Open Public Records Act ("OPRA") request to the Custodian seeking the above-mentioned records. On June 28, 2016, the second (2nd) business day after receipt of the OPRA request, Custodian's Counsel responded in writing on behalf of the Custodian. Therein, Counsel stated that due to the voluminous nature of the OPRA request, the Borough of Point Pleasant ("Borough") Police Department would need 30 to 45 days to respond. Further, Counsel denied access to item No. 6 seeking Officer James Kavanagh's internal disciplinary records under the personnel exemption.

On June 29, 2016, the Complainant responded via e-mail disputing the extension of time. The Complainant contended that his OPRA request sought essentially thirteen (13) items, which should yield only thirteen (13) pages of records.

Denial of Access Complaint:

On July 1, 2016, the Complainant filed a Denial of Access Complaint with the Government

[1] No legal representation listed on record.
[2] Represented by Christopher J. Dasti, Esq., of Dasti, Murphy, McGuckin, Ulaky, Koutsouris & Connors (Forked River, NJ).
[3] The parties may have submitted additional correspondence or made additional statements/assertions in the submissions identified herein. However, the Council includes in the Findings and Recommendations of the Executive Director the submissions necessary and relevant for the adjudication of this complaint.

Records Council ("GRC"). The Complainant contended that the Borough's request for an additional 30 to 45 days to respond to the OPRA request was unreasonable. The Complainant argued that his OPRA request sought thirteen (13) items amounting to the same number of pages of records. The Complainant also disputed the denial of access to item No. 6, but provided no additional arguments regarding the denial.

Supplemental Response:

On July 8, 2016, Custodian's Counsel responded in writing again denying access to item No. 6. Counsel stated that the Police Department was still working to obtain records for request item Nos. 1, 2, 3, 4, 8, and 9. Further, Counsel stated that no records for item Nos. 5, 7, 10, and 11 existed. Counsel also stated that no documents responsive to item Nos. 12 and 13 were in existence at the time of the request and the Custodian was not required to create such per Paff v. Galloway Twp., 44 N.J. Super. 495 (App. Div. 2016).[4] Notwithstanding, Counsel stated that the Police Department was retrieving lists of parking and non-parking tickets issued by officer for the time period indicated in the OPRA request from the municipal court. Counsel stated that he anticipates that the Police Department should be able to respond by the end of the following week.

On July 13, 2016, Custodian's Counsel disclosed ten (10) records to the Complainant. On July 14, 2016, following a conference call with the Complainant, Custodian's Counsel disclosed additional records.

Statement of Information:

On July 21, 2016, the Custodian filed a Statement of Information ("SOI"). The Custodian certified that she received the Complainant's OPRA request on June 24, 2016. The Custodian certified that her search included sending the request to Custodian's Counsel and Police Department. The Custodian noted that the request sought police records and essentially amounted to a discovery request. The Custodian certified that Custodian's Counsel responded on her behalf on June 28, 2016, extending the response time frame 30 to 45 days due to the voluminous nature of the OPRA request. The Custodian further affirmed that she denied access to item No. 6. N.J.S.A. 47:1A-10. The Custodian certified that Counsel disclosed records to the Complainant on July 8, 13, and 14, 2016, while still denying item No. 6 under the personnel exemption.

The Custodian contended that she provided all records that existed and were not otherwise exempt. The Custodian further argued that she lawfully denied access to Officer Kavanagh's personnel file in accordance with N.J.S.A. 47:1A-1.1 and N.J.S.A. 47:1A-10. See Michelson v. Wyatt, 379 N.J. Super. 611 (App. Div. 2005); Merino v. Borough of Ho-Ho-Kus, GRC Complaint No. 2003-110 (March 2004).

[4] The GRC notes that the Supreme Court reversed this decision; thus, requiring agencies to produce electronic information in the form of reports even if the agency was not regularly producing such a report. Paff v. Galloway Twp., 229 N.J. 340 (2017).

Analysis

Timeliness

OPRA mandates that a custodian must either grant or deny access to requested records within seven (7) business days from receipt of said request. N.J.S.A. 47:1A-5(i). A custodian's failure to respond within the required seven (7) business days results in a "deemed" denial. Id. Further, a custodian's response, either granting or denying access, must be in writing pursuant to N.J.S.A. 47:1A-5(g).[5] Thus, a custodian's failure to respond in writing to a complainant's OPRA request either granting access, denying access, seeking clarification or requesting an extension of time within the statutorily mandated seven (7) business days results in a "deemed" denial of the complainant's OPRA request pursuant to N.J.S.A. 47:1A-5(g), N.J.S.A. 47:1A-5(i), and Kelley v. Twp. of Rockaway, GRC Complaint No. 2007-11 (Interim Order October 31, 2007).

In Rivera v. City of Plainfield Police Dep't (Union), GRC Complaint No. 2009-317 (May 2011), the custodian responded in writing to the complainant's request on the fourth (4th) business day by seeking an extension of time to respond and providing an anticipated date by which the requested records would be made available. The complainant did not agree to the custodian's request for an extension of time. The Council stated that:

> The Council has further described the requirements for a proper request for an extension of time. Specifically, in Starkey v. NJ Dep't of Transportation, GRC Complaint Nos. 2007-315, 2007-316 and 2007-317 (February 2009), the Custodian provided the Complainant with a written response to his OPRA request on the second (2nd) business day following receipt of said request in which the Custodian requested an extension of time to respond to said request and provided the Complainant with an anticipated deadline date upon which the Custodian would respond to the request. The Council held that "because the Custodian requested an extension of time in writing within the statutorily mandated seven (7) business days and provided an anticipated deadline date of when the requested records would be made available, the Custodian properly requested said extension pursuant to N.J.S.A. 47:1A-5(g) [and] N.J.S.A. 47:1A-5(i)."

Further, in Criscione v. Town of Guttenberg (Hudson), GRC Complaint No. 2010-68 (November 2010), the Council held that the custodian did not unlawfully deny access to the requested records, stating in pertinent part that:

> [B]ecause the Custodian provided a written response requesting an extension on the sixth (6th) business day following receipt of the Complainant's OPRA request and providing a date certain on which to expect production of the records requested, and, notwithstanding the fact that the Complainant did not agree to the extension of time requested by the Custodian, the Custodian's request for an extension of time

[5] A custodian's written response either granting access, denying access, seeking clarification or requesting an extension of time within the statutorily mandated seven (7) business days, even if said response is not on the agency's official OPRA request form, is a valid response pursuant to OPRA.

[to a specific date] to respond to the Complainant's OPRA request was made in writing within the statutorily mandated seven (7) business day response time.

Moreover, in Werner v. N.J. Civil Serv. Comm'n, GRC Complaint No. 2011-151 (December 2012), the Council again addressed whether the custodian lawfully sought an extension of time to respond to the complainant's OPRA request. The Council concluded that because the Custodian requested an extension of time in writing within the statutorily mandated seven (7) business days and provided an anticipated date by which the requested records would be made available, the Custodian properly requested the extension pursuant to OPRA. In rendering the decision, the Council cited as legal authority Rivera v. City of Plainfield Police Dep't (Union), GRC Complaint No. 2009-317 (May 2011); Criscione v. Town of Guttenberg (Hudson), GRC Complaint No. 2010-68 (November 2010); Rivera v. Union City Bd. of Educ. (Hudson), GRC Complaint No. 2008-112 (April 2010); O'Shea v. Borough of Hopatcong (Sussex), GRC Complaint No. 2009-223 (December 2010); and Starkey v. N.J. Dep't of Transportation, GRC Complaint Nos. 2007-315 through 317 (February 2009).

Although extensions are rooted in well-settled case law, the Council need not unquestioningly find valid every request for an extension containing a clear deadline. In Ciccarone v. N.J. Dep't of Treasury, GRC Complaint No. 2013-280 (Interim Order, dated July 29, 2014), the Council found that the custodian could not lawfully exploit the process by repeatedly rolling over an extension once obtained. In reaching the conclusion that the continuous extensions resulted in a "deemed" denial of access, the Council looked to what is "reasonably necessary."

In the instant matter, the Custodian responded on the second (2nd) business day (through Counsel) seeking an extension of thirty (30) to forty-five (45) days to respond to the Complainant's OPRA request. At that time, the Custodian noted that the request was "voluminous" and "in actuality a discovery request" that should have been sent to the Police Department. The Custodian also denied access to item No. 6, which will be addressed below.

The Complainant's OPRA request, comprised of eight (8) pages, sought thirteen (13) items along with additional dialogue over those pages. The Custodian extended the response time once and ultimately responded on July 13, and 14, 2016 disclosing multiple records. As noted above, a requestor's approval is not required for a valid extension. The GRC notes, however, that the Complainant objected to the Custodian's extension of time prior to filing this complaint.

To determine if the extended time for a response is reasonable, the GRC must first consider the complexity of the request as measured by the number of items requested, the ease in identifying and retrieving requested records, and the nature and extent of any necessary redactions. The GRC must next consider the amount of time the custodian already had to respond to the request. Finally, the GRC must consider any extenuating circumstances that could hinder the custodian's ability to respond effectively to the request.[6]

[6] "Extenuating circumstances" could include, but not necessarily be limited to, retrieval of records that are in storage or archived (especially if located at a remote storage facility), conversion of records to another medium to accommodate the requestor, emergency closure of the custodial agency, or the custodial agency's need to reallocate resources to a higher priority due to *force majeure*.

The evidence of record indicates that the Custodian received this OPRA request, which sought thirteen (13) items and contained extensive dialogue, and believed that it was voluminous and amounted to a discovery request in connection with the Complainant's municipal court action. The Custodian reiterated in the SOI that the extended response time frame was needed due to the voluminous nature of the request. The Custodian also certified that she needed advice from Counsel and had to rely on the Police Department to fulfill the OPRA request. Within two (2) business days following receipt of the OPRA request, the Custodian sought an additional thirty (30) to forty-five (45) days to respond. Thus, the Custodian sought a month or more to respond in addition to the original seven (7) business days. However, the initial time frame would have expired on July 1, 2016 with the extended time frame beginning on July 5, 2016.[7] This is taking into account the remaining five (5) business days after the Custodian's first response. Ultimately, the Custodian only utilized nine (9) calendar days of the extension to complete her response. Thus, in terms of business days, the Custodian's extension only amounted to eight (8) additional business days.

Based on all of the forgoing, the GRC is not persuaded that an additional eight (8) business days was unreasonable given the circumstances of this complaint. The GRC notes that the initial extension of thirty (30) to forty-five (45) calendar days may have bordered on unreasonable. Notwithstanding, the Custodian effectively worked with Counsel and the Police Department to address a rather lengthy thirteen (13) item OPRA request to produce a response within the fifteen (15) business days from receipt of it. Thus, the evidence or record supports that the Custodian reasonably utilized an extension in this complaint.

Accordingly, the Custodian has borne her burden of proof that she timely responded to the Complainant's OPRA request based on a warranted and substantiated extension. N.J.S.A. 47:1A-6. Therefore, no "deemed" denial as it related to the extension occurred in the instant matter. N.J.S.A. 47:1A-5(g); N.J.S.A. 47:1A-5(i).

Unlawful Denial of Access

OPRA provides that government records made, maintained, kept on file, or received by a public agency in the course of its official business are subject to public access unless otherwise exempt. N.J.S.A. 47:1A-1.1. A custodian must release all records responsive to an OPRA request "with certain exceptions." N.J.S.A. 47:1A-1. Additionally, OPRA places the burden on a custodian to prove that a denial of access to records is lawful pursuant to N.J.S.A. 47:1A-6.

OPRA provides that:

> Notwithstanding the provisions [OPRA] or any other law to the contrary, the personnel or pension records of any individual in the possession of a public agency, including but not limited to records relating to any grievance filed by or against an individual, shall not be considered a government record and shall not be made available for public access . . .
>
> [N.J.S.A. 47:1A-10.]

[7] July 4, 2016 was a federal holiday and thus not included in the "business day" calculation.

OPRA begins with a presumption against disclosure and "proceeds with a few narrow exceptions that . . . need to be considered." Kovalcik v. Somerset Cnty. Prosecutor's Office, 206 N.J. 581, 594 (2011). These are:

> [A]n individual's name, title, position, salary, payroll record, length of service, date of separation and the reason therefore, and the amount and type of any pension received shall be government record;
>
> [P]ersonnel or pension records of any individual shall be accessible when required to be disclosed by another law, when disclosure is essential to the performance of official duties of a person duly authorized by this State or the United States, or when authorized by an individual in interest; and
>
> [D]ata contained in information which disclose conformity with specific experiential, educational or medical qualifications required for government employment or for receipt of a public pension, but not including any detailed medical or psychological information, shall be a government record.
>
> [Id.]

The Council has addressed whether personnel records not specifically identified in OPRA were subject to disclosure. For instance, in Guerrero v. Cnty. of Hudson, GRC Complaint No. 2010-216 (December 2011), the complainant sought, among other records, "[a]ny known felony charges." Id. In the SOI, the custodian argued that he was precluded from acknowledging the existence of felony charges because such information is not included within the excepted personnel information under OPRA. The Council agreed, determining that ". . . even if records of any felony charges were contained within Mr. Spinello's personnel file, such records are not disclosable under OPRA . . ." Id. at 8. The Council reasoned that "OPRA clearly identifies certain [personnel] information that is subject to disclosure . . . These exceptions do not include any possible felony or criminal charges . . . Thus, OPRA implies that personnel records referencing felony charges are not subject to disclosure . . ." Id.

Further, the Council has determined that records involving employee discipline or investigations into employee misconduct are properly classified as personnel records exempt from disclosure under N.J.S.A. 47:1A-10. In Merino v. Borough of Ho-Ho-Kus, GRC Complaint No. 2003-110 (March 2004), the Council found that records of complaints or internal reprimands against a municipal police officer were properly classified as personnel records encompassed within the provisions of N.J.S.A. 47:1A-10. For this reason, the Council concluded that ". . . records of complaints filed against [the police officer] and/or reprimands [the officer] received are not subject to public access." Id.; See also Wares v. Twp. of West Milford (Passaic), GRC Complaint No. 2014-274 (May 2015).

Here, the Complainant's OPRA request item No. 6 sought records in connection with "complaints or concerns" raised about Officer Kavanagh. The Custodian initially responded, and later restated in the SOI, that the request was denied under N.J.S.A. 47:1A-10. The Council's decisions support such a denial: the facts here are on square with Merino, GRC 2003-110 and all

relevant progeny. Specifically, the records sought here relate to complaints filed against Officer Kavanagh, as was the case in Merino. For this reason, the GRC is satisfied that the Custodian lawfully denied access to any records responsive to the Complainant's OPRA request item No. 6.

Accordingly, the requested records in connection with "complaints and concerns" raised about Officer Kavanagh are exempt from disclosure as "personnel records." N.J.S.A. 47:1A-10; Merino, GRC 2003-110. See also Wares, GRC 2014-274. Thus, the Custodian lawfully denied access to item No. 6 of the Complainant's OPRA request. N.J.S.A. 47:1A-6.

Conclusions and Recommendations

The Council Staff respectfully recommends the Council find that:

1. The Custodian has borne her burden of proof that she timely responded to the Complainant's OPRA request based on a warranted and substantiated extension. N.J.S.A. 47:1A-6. Therefore, no "deemed" denial as it related to the extension occurred in the instant matter. N.J.S.A. 47:1A-5(g); N.J.S.A. 47:1A-5(i).

2. The requested records in connection with "complaints and concerns" raised about Officer Kavanagh are exempt from disclosure as "personnel records." N.J.S.A. 47:1A-10; Merino v. Borough of Ho-Ho-Kus, GRC Complaint No. 2003-110 (March 2004). See also Wares v. Twp. of West Milford (Passaic), GRC Complaint No. 2014-274 (May 2015). Thus, the Custodian lawfully denied access to item No. 6 of the Complainant's OPRA request. N.J.S.A. 47:1A-6.

Prepared By: Frank F. Caruso
Communications Specialist/Resource Manager

March 20, 2018

OPRA and Electronically Stored Information Hold/Litigation Hold

Dear Point Pleasant borough clerk,

I, Marc Mayer, in connection with ticket number 001068 involving Officer J Kavanaugh. On June 22, 2016, I was stopped by Officer Kavanaugh who issued a summons against me under 39:4-98.

FOIA Request

Pursuant to the New Jersey OPRA Act (FOIA), I demand that you submit the following information/documents to me:

1. Any and all videotape from every onboard and/or body camera of every police vehicle and officer corresponded to incident on June 22, 2016.

2. Any and all audio tapes, audio tracks, audio recordings, or transcripts of all police radio traffic taken on June 22, 2016 related to Officer Kavanaugh and I, Marc Mayer, including but not limited to all radio traffic from the time Officer Kavanaugh pursued I, Marc Mayer until I was released and all communication related to I, Marc Mayer ended (hereinafter referred to as the "Mayer incident").

3. Any and all police dispatch logs related to the Mayer incident (June 22, 2016).

4. A copy of the original summons under 39:4-98.

5. Any and all police notices or advisories related to Marc Mayer held by the Point Pleasant Police.

6. Records specifically concerning Officer Kavanaugh kept pursuant to NJ Code, including without limitation any personnel records, any documents collected, created, or maintained in connection with complaints or concerns raised about Officer Kavanaugh's behavior or conduct, and any documents collected, created, or maintained in connection with any investigations into Officer Kavanaugh's behavior or conduct.

7. The number of records responsive to each of the above requests that are being withheld, and the specific basis for each such records being withheld.

8. Calibration records for any speed detection equipment used by Officer Kavanaugh in regards to the issuance of 39:4-98

8b. Radar/Laser device maintenance records

8c. Tuning fork calibration records

9. The Operator's Manuals for any speed detection equipment used by Officer Kavanaugh in regards to the issuance of 39:4-98.

10. The Point Pleasant Police Department regulations and guidelines regarding the use, operation, and policies for the use of speed detection equipment.

11. All engineering reports and studies performed in the determination of the posted limit, to include, but not limited to, the most recent 85th percentile speed measurement and any collision data used in the determination of the posted limit (as required by Federal law).

> When this State took one cent of Federal Highway funds it agreed in writing to give sovereignty of the roads to the Federal Government. Every municipality that has taken one cent of State money by agreement in return for this money has subrogated itself to the Federal Government. The only legal authority for speed enforcement is under the color of Federal Law even in the enforcement of local speed ordinances. The prosecution has two choices under 23 CFR and MUTCD Title 23; Produce the engineering survey or produce documentation that this State, Township or Municipality has never received one cent of State or Federal Highway or road funds.

12. A listing of traffic tickets issued by Officer Kavanaugh for the month of June 2016, to include: date and time issued, alleged violation, and disposition, (if determined).

13. A total tally of all traffic tickets issued by the Point Pleasant Police Department for the month of June 2016, to include: date issued, alleged violation, the DSN of the issuing officer, and disposition, (if determined).

Pursuant to OPRA guidelines I demand all documents be emailed and NOT printed on physical media. Pursuant to N.J.S.A. 47:1A-5.b. "OPRA was amended to allow the production of electronic records FREE OF CHARGE, except that a public agency may charge the actual cost of any needed supplies such as computer discs."

ALL denied records will be challenged via suit in Superior Court filed within the allotted 45 days. In accordance with OPRA "Successful plaintiffs may be entitled to reasonable attorney fees," and all will be sought.

Electronically Stored Information ("ESI") Hold Litigation Hold of ESI

Additionally, I, Marc Mayer demand that you preserve all documents, tangible things and electronically stored information potentially relevant to his claims arising out of the stop on June 22, 2016 and subsequent prosecution, including but not limited to:

1. Any and all documents which describe actions taken by Officer Kavanaugh against me, Marc Mayer;
2. Any and all communications by the Point Pleasant Police department about me, Marc Mayer;

3. Any and all communications by any party concerning me, Marc Mayer and/or the interaction between Officer Kavanaugh and I and/or the court and/or the Attorney's office;
4. Any and all documents related to any actions or conduct of any officers involved in my (Marc Mayer) stop, detention, issuance of summons, and/or prosecution;
5. Internal Investigations related to the Mayer incident;
6. Any discipline arising out of the Mayer incident.

As used in this demand, "you" and "your" refers to the Point Pleasant Police Department, its successors, divisions, affiliates, and its officers, directors, agents, attorneys, committees, accountants, employees, 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, should the matter proceed to litigation, 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 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 messaging);
- 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., OuickBooks, 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, SOL 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.

Preservation Requires Immediate Intervention

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), you 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 the 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 the plaintiff of his right to secure the evidence or the Court of its right to adjudicate the issue.

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 22, 2016, through the date of this demand and continuing and concerning issues or allegations related to the issues set forth above including but not limited to:

1. Any and all e-mails and other electronic communications made or received related to the Mayer incident;
2. Any and all e-mails and other electronic communications, statements or correspondences made by any officers responding to the Mayer incident;
3. Any and all electronic records of statements or correspondences made by the responding officers amongst each other;
4. Any and all documents related to the Mayer incident;

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 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:

- 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 1M 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'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 identified 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 that person during the period from June 22, 2016, to the present and continuing, 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 the litigation. 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 10 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 OVO 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 must notify any current or former agent, attorney, 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

I suggest that, with respect to all of the police officers involved in the Mayer incident, 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

I am 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

I'm 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 sanctions.

Confirmation of Compliance

Please confirm 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, please describe what you have done to preserve potentially relevant evidence.

I look forward to your prompt response.

Marc Mayer
24 Carnegie Street
South Toms River, NJ 08757

Phone: 908-814-8246
Email: BlindSk8er82489@gmail.com

_____ _____

Marc Mayer Date

_____ _____

Pt. Pleasant Borough Clerk: Antoinette Jones, RMC, CMR Date