

# **EXHIBIT 6**

# Expert Report of Brandon Leatha

## Regarding the Inspection of Certain City-Issued Cellular Telephones Used by Specific City of Seattle Officials

Hunters Capital, et al. v. City of Seattle  
Case No. 20-983 TSZ (W.D. Wash.)

### Table of Contents

---

1	Background & Materials Considered .....	2
2	Qualifications .....	2
3	Summary of Findings.....	3
4	Device Summary .....	6
5	Text Message Retention Settings.....	7
6	Communication Applications .....	9
7	Evidence of Devices Having Been Factory Reset .....	9
8	Evidence of Failed Credentials .....	9
9	Evidence of File Deletion.....	10
10	Evidence of Data Wiping and Hiding.....	11
11	Evidence of ESI Available from Other Sources.....	11
12	Assessment of Forensic Extractions and Backups.....	11
13	Evaluation of Devices Used by City Officials .....	12
13.1	Former Mayor Durkan .....	12
13.2	Former Chief Best .....	15
13.3	Chris Fisher.....	17
13.4	Kenneth Neafcy.....	20
13.5	Chief Scoggins .....	23
13.6	Idris Beauregard.....	25
13.7	Assistant Chief Greening.....	27

## 1 Background & Materials Considered

---

I was retained by counsel for Plaintiffs in this action to provide expert digital forensics services related to the analysis of electronically stored information (“ESI”) produced by the City of Seattle, and to report on and provide testimony about my findings.

I understand that Hunters Capital filed a lawsuit against the City of Seattle (“City”) on June 24, 2020, and sent letters on June 27 and June 30 requesting the preservation of text messages, among other types of ESI. The City disclosed that it was unable to produce some or all text messages for certain City officials (“City Officials”). On October 19, 2021, the Court ordered the City to provide the data collected from the impacted City Officials’ cellphones, including Mayor Jenny Durkan, former Police Chief Carmen Best, Fire Chief Harold Scoggins, Idris Beauregard, Christopher Fisher, Ken Neafcy, and Eric Greening. On October 31, 2021, the City’s vendor provided the data collected from each of the seven City Officials’ cellphones and associated cloud accounts. This report details the results of my analysis of the cellphone data provided and the availability of text messages for each of the City Officials.

In preparation of this report and my opinions expressed herein, I have relied on my training, education, and over 22 years of experience performing eDiscovery and digital forensic investigations. The materials that I have considered include certain text message productions made by the City, the FRCP 26(a)(2)(B) Expert Report of Kevin T. Faulkner, letters and interrogatory responses from the City, deposition transcripts, and the forensic extractions and backups of cellular phones and associated cloud accounts used by the City Officials. A list of the materials that I have considered is included as Exhibit A to this report and a table with details about the source devices that I analyzed is included in the “Device Summary” section below.

I am being compensated at an hourly rate of \$450 for my services. My work in this matter is ongoing and I reserve the right to update my report and opinions as I continue my investigation or receive new information.

## 2 Qualifications

---

I am the Founder and CEO of Leatha Consulting LLC, an expert services and consulting firm that provides digital forensics, electronic discovery, expert testimony, and technology consulting services. Prior to my current role, I was a Director at iDiscovery Solutions (“iDS”) and the Director of ESI Consulting and Data Analysis at Electronic Evidence Discovery (“EED”).

I have more than 22 years of experience performing digital forensic investigations, incident response, and electronic discovery services. I provide services and consult with clients on the collection, preservation, analysis, and production of electronically stored information. I have extensive experience and expertise in the examination of email, documents, and other electronically stored information (“ESI”) in a litigation context, including ESI maintained on personal computers, servers, enterprise applications, databases, cellular phones, tablets, mobile devices, IOT devices, cloud storage applications, social media, and other internet-based services.

I have a Bachelor of Arts in Environmental Studies from the University of Washington, a certificate in Computer Forensics from the University of Washington, and I am a GIAC Certified Forensic Examiner (“GCFE”) and GIAC Certified Incident Handler (“GCIH”).

I am on the Board of Directors of the Computer Technology Investigators Network (“CTIN”), the Board Vice President of the Puget Sound chapter of the Information Systems Security Association (“ISSA”), and on the Advisory Board for the SANS Institute’s Global Information Assurance Certification (“GIAC”) program. I have been a member of the Sedona Conference since 2005 and have participated in the Working Groups on Electronic Document Retention and Production (“WG1”) and Data Security and Privacy Liability (“WG11”).

I have testified in both state and federal cases as a fact witness, as a FRCP Rule 30(b)(6) witness, and as an FRCP 26(a)(2)(B) expert witness. I have provided electronic discovery and digital forensics services to both plaintiffs and defendants, and I have been a court appointed neutral expert. My qualifications as well as a list of the cases for which I have testified are included in my CV attached as Exhibit B to this report.

### 3 Summary of Findings

---

I have analyzed the information collected from the cellphones of the seven City Officials and found that actions taken after the lawsuit was filed resulted in a significant loss of text messages from each of their cellphones. The post-lawsuit actions which resulted in the loss of text messages include the following:

#### **Mayor Jenny Durkan**

- Mayor Jenny Durkan’s iPhone 8 Plus (FirstNet) was factory reset on July 4, 2020, and again on September 17, 2020. See “Factory Reset (former Mayor Durkan)” section below.
- Mayor Jenny Durkan’s iPhone was configured to automatically delete text messages older than 30-days. Her text message retention settings were changed from “Forever” to “30 Days” sometime between July 4, 2020, and July 26, 2020. See “Text Message Retention Settings (former Mayor Durkan)” section below.
- All of Mayor Jenny Durkan’s text messages were deleted from her iCloud account using the “Disable & Delete” function on July 4, 2020. See “Evidence of File Deletion (former Mayor Durkan)” section below.
- 5,937 text messages were deleted from Mayor Jenny Durkan’s iPhones between July 4, 2020, and November 16, 2020. Of the 5,937 deleted text messages, 191 were deleted manually and were not the result of the 30-day message retention setting. See “Evidence of File Deletion (former Mayor Durkan)” section below.

### **Chief Carmen Best**

- Chief Carmen Best's iPhone was configured to automatically delete text messages older than 30-days. See "Text Message Retention Settings (former Chief Best)" section below.
- 27,138 text messages were deleted from Chief Carmen Best's iPhone. When her phone was returned to the City on or around September 2, 2020, only 15 text messages remained on the device. See "Evidence of File Deletion (former Chief Best)" section below.

### **Chris Fisher**

- Chris Fisher's iPhone was configured to automatically delete text messages older than 30-days. See "Text Message Retention Settings (Chris Fisher)" section below.
- 15,843 text messages were deleted from Chris Fisher's iPhone. When the City collected data from his iPhone 7 on February 22, 2021, only 16 messages remained on the device. See "Evidence of File Deletion (Chris Fisher)" section below.
- Chris Fisher's iPhone 7 was restored from a backup on November 3, 2020, a process which first requires the phone to be erased, or factory reset. See "Evidence of Devices Having Been Factory Reset (Chris Fisher)" section below.
- Chris Fisher used at least two other iPhones between June 1, 2020, and October 31, 2020, neither of which were disclosed in response to the October 19, 2021, Stipulated Digital Examination Agreement and Order. See "Evidence of ESI Available from Other Sources (Chris Fisher)" section below.

### **Ken Neafcy**

- Ken Neafcy's iPhone XS was factory reset on October 27, 2020, resulting in the loss of all text messages dated between March 19, 2020, and October 28, 2020. See "Evidence of Devices Having Been Factory Reset (Kenneth Neafcy)" section below.

### **Chief Harold Scoggins**

- Chief Harold Scoggins iPhone 8 Plus was factory reset on October 8, 2020, resulting in the loss of all text messages prior to that date. See "Evidence of Devices Having Been Factory Reset (Chief Scoggins)" section below.

### **Idris Beauregard**

- Idris Beauregard's iPhone 8 was factory reset on October 9, 2020, resulting in the loss of all text messages prior to that date. See "Evidence of Devices Having Been Factory Reset (Idris Beauregard)" section below.

**Asst. Chief Eric Greening**

- Asst. Chief Eric Greening’s Samsung Galaxy S8 was factory reset on approximately October 26, 2020, resulting in the loss of all text messages prior to that date. See “Assistant Chief Greening” section below.

The actions outlined above each resulted in the loss of text messages that the City had an obligation to preserve. If a technical issue prevented the City Officials from accessing their phones, a temporary replacement should have been issued instead of factory resetting and deleting all the data. A qualified digital forensic vendor could then have assisted with preserving the data. The following timeline shows the events which resulted in the loss of text messages for each of the seven City Officials. See Figure 1 below.

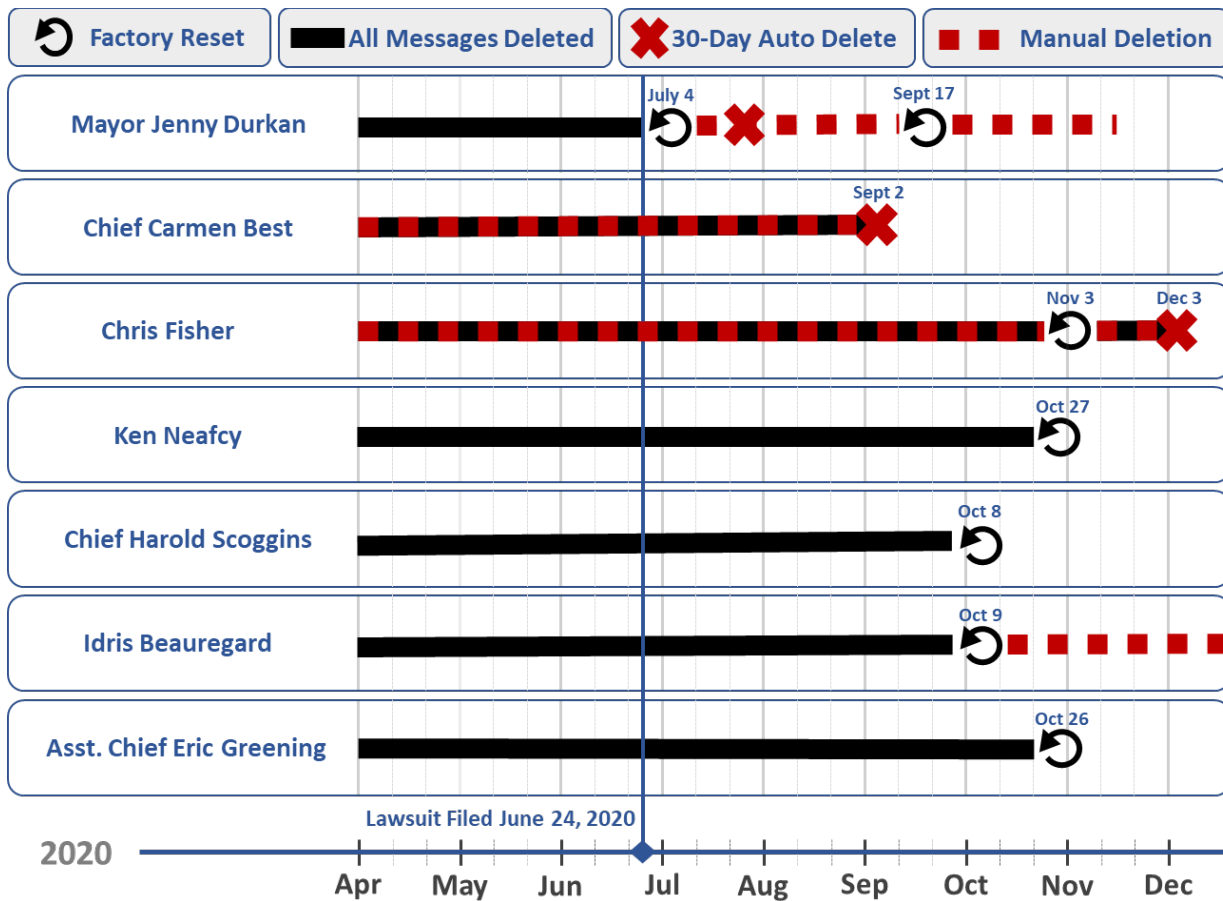


Figure 1. Timeline of events resulting in the loss of text messages

## 4 Device Summary

On October 31, 2021, I received notice from Kevin Faulkner of Palo Alto Networks Unit 42, one of the City's forensic vendors, that forensic extractions and backups of cellular phones used by certain City Officials were available for me to download from a secure network location. I completed the download of approximately 114GB of data, which included backups, forensic extractions, and other information about the cellular phones outlined in the DEA. On November 1, 2021, the City provided an "ESI Log" which included additional details about the forensic extractions and backups provided by the City. The following table summarizes the data provided by the City. See figure 2.

Evidence ID	Custodian	Extraction Type <sup>1</sup>	Source Date <sup>2</sup>	Source Description
E033A	Beauregard, Idris	CB Adv Logical	3/9/2021	Apple iPhone 8; SN: <b>Redacted</b>
E055A	Beauregard, Idris	Elcomsoft EPB	10/28/2021	iCloud Backup
E055B	Beauregard, Idris	Elcomsoft EPB	10/28/2021	iCloud Synced
E055C	Beauregard, Idris	Elcomsoft EPB	10/28/2021	iCloud Synced
E009A	Best, Carmen	CB Adv Logical	2/24/2021	iPhone XS Max; SN: <b>Redacted</b>
E004A2	Durkan, Jenny	iTunes Backup	8/29/2019	iPhone 8 Plus (Verizon); SN: <b>Redacted</b>
E004A1	Durkan, Jenny	iTunes Backup	8/21/2020	iPhone 11 (FirstNet); SN: <b>Redacted</b>
E002A	Durkan, Jenny	Magnet Acquire	9/18/2020	iPhone 8 Plus (FirstNet); SN: <b>Redacted</b>
E003A	Durkan, Jenny	Magnet Acquire	10/15/2020	iPhone 11 (FirstNet); SN: <b>Redacted</b>
E001A	Durkan, Jenny	Axiom Cloud	11/16/2020	iCloud Files; Apple ID: <b>Redacted</b>
E001B	Durkan, Jenny	Elcomsoft EPB	11/16/2020	iCloud Backup; Apple ID: <b>Redacted</b>
E001C	Durkan, Jenny	Elcomsoft EPB	11/16/2020	iCloud Synced; Apple ID: <b>Redacted</b>
E001D	Durkan, Jenny	Elcomsoft EPB	11/16/2020	iCloud Files; Apple ID: <b>Redacted</b>
E005A	Durkan, Jenny	CB Adv Logical	11/19/2020	iPhone 8 Plus (FirstNet); SN: <b>Redacted</b>
E008A	Durkan, Jenny	CB Adv Logical	11/19/2020	iPhone 11 (FirstNet); SN: <b>Redacted</b>
E010A	Durkan, Jenny	CB Adv Logical	7/2/2021	iPhone 8 Plus (Verizon); SN: <b>Redacted</b>
E005C	Durkan, Jenny	CB Full FS	7/7/2021	iPhone 8 Plus (FirstNet); SN: <b>Redacted</b>

<sup>1</sup> The City and its vendors utilized specialized software to download, backup, or extract information from the City's cellphones and accounts. The extraction type describes the type of data backed up and the software or method used for the backup.

<sup>2</sup> The Source Date reflects when the backup, download, or extraction was created and does not necessarily reflect when the specific device was last used.

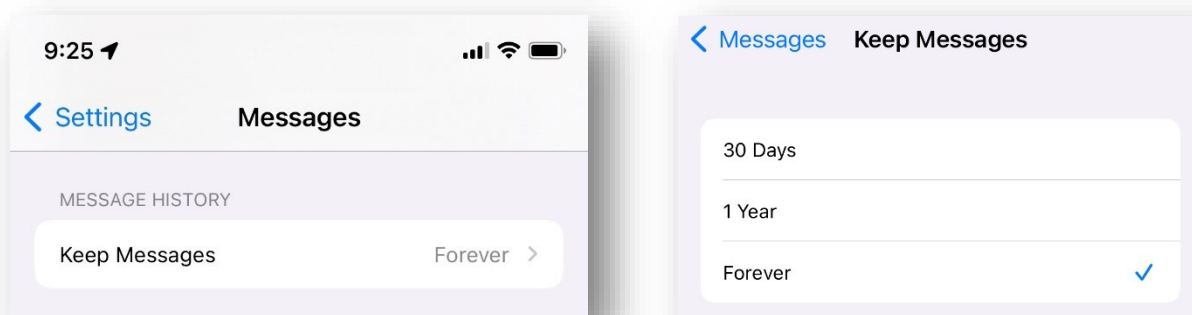
E010B	Durkan, Jenny	CB Full FS	7/7/2021	iPhone 8 Plus (Verizon); SN: <b>Redacted</b>
E008B	Durkan, Jenny	Belkasoft Full FS	7/8/2021	iPhone 11 (FirstNet); SN: <b>Redacted</b>
E047B	Durkan, Jenny	Elcomsoft EPB	9/9/2021	iCloud Synced; Apple ID: <b>Redacted</b>
E016A	Fisher, Christopher	CB Adv Logical	2/22/2021	Apple iPhone 7; SN: <b>Redacted</b>
E022A	Greening, Eric	CB Adv Logical	3/1/2021	Samsung Galaxy S8; IMEI: <b>Redacted</b>
E054A	Greening, Eric	CB Adv Logical	10/27/2021	Samsung Galaxy S8; IMEI: <b>Redacted</b>
E054B	Greening, Eric	CB Full FS	10/27/2021	Samsung Galaxy S8; IMEI: <b>Redacted</b>
E050	Neafcy, Ken	iTunes Backup	3/1/2021	iPhone 6s; SN: <b>Redacted</b>
E045A	Neafcy, Ken	iTunes Backup	8/17/2021	iPhone XS; SN: <b>Redacted</b>
E049A	Neafcy, Ken	Passware Full FS	10/27/2021	iPhone 6s; SN: <b>Redacted</b>
E056A	Neafcy, Ken	Elcomsoft EPB	10/28/2021	iCloud Backups; Apple ID: <b>Redacted</b>
E056B	Neafcy, Ken	Elcomsoft EPB	10/28/2021	iCloud Synced; Apple ID: <b>Redacted</b>
E056C	Neafcy, Ken	Elcomsoft EPB	10/28/2021	iCloud Files; Apple ID: <b>Redacted</b>
E049B	Neafcy, Ken	CB Adv Logical	10/30/2021	iPhone 6s; SN: <b>Redacted</b>
E052A	Scoggins, Harold	Elcomsoft EPB	2/13/2021	Apple iPhone 8 Plus (iCloud Backup); SN: <b>Redacted</b>
E052B	Scoggins, Harold	Elcomsoft EPB	2/16/2021	Apple iPhone 8 Plus (iCloud Backup); SN: <b>Redacted</b>
E051	Scoggins, Harold	iTunes Backup	3/9/2021	Apple iPhone 11; SN: <b>Redacted</b>

**Figure 2. Table of forensic extractions and backups provided by the City**

## 5 Text Message Retention Settings

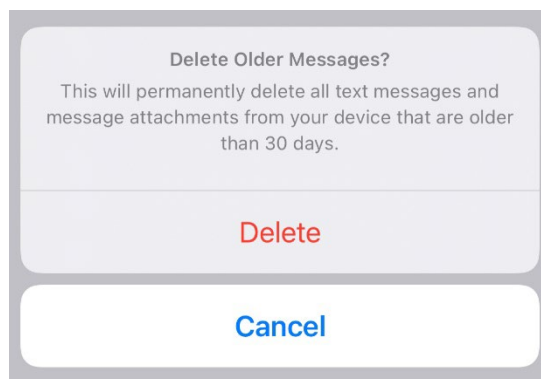
Certain settings can be applied to cellphones which affect the retention of text messages, iMessage chat, and other electronic chat messages. By default, an Apple iPhone retains messages indefinitely. However, a user can configure the iPhone to delete all messages older than 30 days, or all messages older than one year. To change the settings, the user must select *Settings > Messages > Keep Messages*, and change the setting from “Forever”, to “30 days” or “1 Year”. See Figure 3.





**Figure 3. iPhone message retention settings**

When the user changes the setting from “Forever” to “30 Days” or “1 Year”, a warning message notifies the user that older messages will be permanently deleted. The user can then choose to “Cancel” or confirm the change by selecting the “Delete” option. See Figure 4.



**Figure 4. Warning message seen when the iPhone message retention setting is changed**

Once the setting has been applied, messages that meet the specified age will continue to be deleted, or “expire”, nightly on a rolling basis. Even if the “Keep Messages” configuration is set to “Forever” a user can still manually delete messages and conversation threads.

The current message retention setting, as well as the number of times the message retention setting has been changed, are stored in the **com.apple.MobileSMS.plist** configuration file. The current message retention setting is stored in a key named **KeepMessageForDays**, and the values are “0” for Forever, “30” for 30 Days, and “365” for 1 Year retention. The number of times the phone’s message retention setting has been changed is stored in a key named **KeepMessagesVersionID**. While the phone does track how many times the message retention setting was changed, it does not track when the settings were changed or what the prior values were. If the **KeepMessageForDays** and **KeepMessagesVersionID** are not found in the **com.apple.MobileSMS.plist** configuration file, this indicates that the phone was configured with the default “Forever” retention setting.

If a user gets a new iPhone, they can optionally transfer certain settings and data from their prior phone. If this is done, the **KeepMessageForDays** retention setting and **KeepMessagesVersionID** are typically

transferred to the new phone. The City's forensic expert, Kevin Faulkner, investigated other configuration changes that can be made to an iPhone that may also cause the **KeepMessagesVersionID** value to increment by 1. For example, when turning "Messages in iCloud" on or off, the **KeepMessagesVersionID** is incremented by 1. See Faulkner, 20-21.

## 6 Communication Applications

---

Cell phones and other mobile devices support various forms of communication, including email, text, chat, voice and video. Apple iPhones and Android phones typically include standard applications for sending and receiving email, text messages, and phone calls. However, a user can install any number of additional communications applications, including applications for services such as Facebook Messenger, Skype, Signal, and Telegram, among others. Each of the backups provided by the City were evaluated to determine which communication applications were installed and used.

## 7 Evidence of Devices Having Been Factory Reset

---

When a phone is factory reset, all the data maintained on the device is deleted and is irrecoverable from the reset device. When an Apple iPhone is factory reset, the phone automatically restarts after the reset process completes. Examining certain forensic artifacts on the reset phone can provide information about when the reset process finished and the phone first restarted.<sup>3</sup>

Depending on the type of backup or forensic extraction, some of the artifacts may not be present. A 0 byte file named **.obliterated** is typically created in the **/private/var/root** folder of an iPhone that has been factory reset. The date that the **.obliterated** file was created reflects when the iPhone first started after the factory reset process. A configuration file named **com.apple.purplebuddy.plist** contains entries about when an iPhone was first set up, including the setup activities which occur after a factory reset. The **GuessedCountry**<sup>4</sup> key typically reflects when the setup process began, and the **SetupLastExit** key typically reflects when the setup process was completed. In some cases, an iPhone can be used without the setup process being completed, and thus the **SetupLastExit** date may be later than the **GuessedCountry** key. The first entries in the **ZPROCESS** and **ZLIVEUSAGE** tables from the **DataUsage.sqlite** typically reflect the first activities on the iPhone after it first restarts. Additionally, the dates that certain database and configuration files were created can be used to confirm when the device was first restarted after a factory reset.

## 8 Evidence of Failed Credentials

---

Access to iPhones can optionally be protected by a passcode. If a passcode is set, certain iPhone models support "Touch ID", which unlocks the device with a fingerprint, or "Face ID", which unlocks the device with facial recognition. If a user forgets a password or passcode, it may not be possible for the user to

---

<sup>3</sup> A Cellebrite blog article that describes various methods to determine if and when an iPhone was factory reset can be found at: <https://cellebrite.com/en/upgrade-from-null-detecting-ios-wipe-artifacts/>

<sup>4</sup> The **GuessedCountry** key from the **com.apple.purplebuddy.plist** configuration file contains a sub-key named "at" which stores the date that the "Country or Region" information is selected during the iPhone setup process.

access the information on the device or account. The City reported that multiple City Officials forgot the passcode to their iPhones and became locked out. In all instances, the iPhones were factory reset prior to being sent to a forensic vendor for inspection and forensic extraction, and thus no data was available which could confirm the events that occurred prior to the phones being factory reset. Depending on the model of iPhone and the version of the iOS operating system, certain software and forensic services could have bypassed the screen lock to gain access to and preserve the data stored on the phone.

## 9 Evidence of File Deletion

---

As described in the “Text Messages Retention Settings” section above, an iPhone can be configured to automatically delete text messages after 30 days or after one year. The user can also manually delete text messages by selecting individual messages or by selecting an entire conversation thread. An inspection of the information remaining in the iPhone’s **sms.db** text message database can provide details about the deletion events, such as how many messages were deleted, the time period of the deleted messages, and possibly how the messages were deleted.

The City’s expert provides a detailed explanation describing how to determine if a message deletion was performed by the configured “30 day” message retention setting, by the user selecting individual messages to delete, or by the user deleting an entire conversation thread. If the chat entry exists without any associated messages, the message deletion was performed by the configured retention setting or by manually deleting individual messages. However, if the chat entry is missing, the entire conversation thread was manually deleted by the user. See Faulkner, 23-24.

One can also use the ROWID in the **message** and **chat** tables in the **sms.db** to identify “gaps” or missing messages and conversation threads. When messages are sent or received by an iPhone, they are stored sequentially in the **message** table, where each subsequent message receives the next **ROWID**<sup>5</sup>. Likewise, each new chat is assigned the next available **ROWID**. By identifying the gaps in the sequential **ROWID** found in the **message** and **chat** tables, one can determine how many messages and chats are missing. One can also use the date of the preceding and subsequent messages to determine a date range for the missing message(s). The deleted messages identified using this process were manually deleted, either by selecting individual messages or by selecting an entire conversation thread at a time. If the messages were deleted by the iPhone message retention settings, all messages older than the configured expiration date (“30 days” or “1 Year”) would be missing and the gaps would not exist.

The **sqlite\_sequence** table in the **sms.db** keeps track of the next available ID for certain tables. The **seq** column stores the next available **ROWID** for the **deleted\_messages** and **sync\_deleted\_messages** tables, and the current value reflects the number of messages and chats that have been deleted from the phone. The number of “missing” or deleted chats and messages can also be confirmed by subtracting the number of entries found in the chat and message tables from the maximum **ROWID** in each table.

---

<sup>5</sup> The City’s expert provides a detailed description about when messages are restored from iCloud, the restored messages are downloaded from newest to oldest, and thus the message **ROWID** in the **sms.db** would be assigned in reverse order. See Faulkner, 29. However, after the historic messages were restored iCloud, new messages sent or receive from the iPhone would be assigned the next greater **ROWID** for each new message.

## 10 Evidence of Data Wiping and Hiding

---

When an iPhone is factory reset, the device is essentially “wiped”, and the data cannot be recovered from the device directly. Details regarding the factory reset process for each device is discussed in the “Evaluation of Devices Used by City Officials” section below.

I did not find evidence that specialized software or applications were used to wipe or hide information from the devices subject to the DEA.

## 11 Evidence of ESI Available from Other Sources

---

Information from iPhones and other mobile devices can be stored in many locations, including iCloud backups, iTunes backups, prior forensic extractions, previously used devices, and information synchronized to other devices, such as an iPad or Apple computer connected to the same iCloud account.

When information is downloaded from a user’s iCloud account using the Elcomsoft forensic software, information about each device connected to the same iCloud account is saved in the **devices.json** and **trusted\_devices.json** file. Evaluating this information may show that other devices were connected to the same iCloud account and could have data, such as text messages, synchronized to the device.

By inspecting certain configuration files found in an iPhone backup, one can determine when the device was last backed up. The **com.apple.madrid.plist** configuration file includes keys such as **CloudKitInitialStartDate**, which tracks when the device was first configured to store “Messages in iCloud”, and **CloudKitSyncingEnabled**, which tracks if the phone was configured to store “Messages in iCloud” at the time the device was backed up. The **com.apple.mobile.lidbackup.plist** configuration file includes keys such as **LastiTunesBackupDate**, which indicates the date of the last iTunes backup, **LastCloudBackupDate**, which indicates the date of the last iCloud backup, and **CloudBackupEnabled**, which indicates if iCloud backups were enabled. If “Messages in iCloud” was enabled at the time of an iCloud backup, the messages are excluded from the backup. Conversely, if “Messages in iCloud” is not enabled at the time of a backup, the backup includes the messages from the device. The **iTunesPrefs** file contains names of computers that the device had be previously connected to, as well as the computer’s “user account” in use when the device was connected. This forensic artifact can be used to identify computers that may contain the contents of prior iTunes backups.

## 12 Assessment of Forensic Extractions and Backups

---

This section evaluates the methods used by the City and its vendors to backup or extract information from the City officials’ phones, cloud accounts, and other sources of ESI. A variety of methods exist to backup or extract information from iPhones, iCloud accounts, and other mobile devices. Some methods provide a more complete forensic backup, typically referred to as a full file system extraction, but these use specialized software and may require the use of “jailbreak” software to bypass the device security.

The timing of when information is downloaded from iCloud accounts is important because backups and synchronized data can expire or be overwritten. Apple typically saves the two most recent backups for a

configured device, and each time a new backup is created, the oldest backup is eliminated. If a device is no longer backed up to iCloud, Apple typically deletes the last remaining backup after 180 days. If the “Messages in iCloud” feature was once enabled, and subsequently disabled, the messages would be available in iCloud for 30 days after the feature was turned off.

## 13 Evaluation of Devices Used by City Officials

### 13.1 Former Mayor Durkan

#### Text Message Retention Settings (former Mayor Durkan)

The City provided backups for three different iPhones used by Durkan between April 10, 2018 and November 19, 2020. At the time each of the backups was created, the phone was configured to retain messages forever. However, the City’s forensic expert concluded that sometime between July 4, 2020, and July 26, 2020, Durkan’s iPhone was configured to delete all messages older than 30 days. See Faulkner, 33-34. Faulkner was not able to determine if the 30-day retention setting was first applied on the iPhone 8 Plus (FirstNet) that Durkan used until July 9, 2020, or the iPhone 11 (FirstNet) that replaced it. The following table provides additional detail about the text message retention settings found on each of Durkan’s iPhone backups provided by the City. See figure 5.

Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone 8 Plus (Verizon)	4/10/2018	10/30/2019	8/29/2019	Forever	0
iPhone 8 Plus (Verizon)	4/10/2018	10/30/2019	7/2/2021	Forever	1
iPhone 8 Plus (Verizon)	4/10/2018	10/30/2019	7/7/2021	Forever	1
iPhone 8 Plus (FirstNet)	10/30/2019	7/9/2020	9/18/2020	Unknown, Phone was factory reset	
iPhone 8 Plus (FirstNet)	10/30/2019	7/9/2020	11/19/2020	Unknown, Phone was factory reset	
iPhone 8 Plus (FirstNet)	10/30/2019	7/9/2020	7/7/2021	Unknown, Phone was factory reset	
iPhone (unknown)	Between 7/4/2020 and 7/26/2020			30	3
iPhone 11 (FirstNet)	7/9/2020	11/19/2020	8/21/2020	Forever	4
iPhone 11 (FirstNet)	7/9/2020	11/19/2020	10/15/2020	Forever	4
iPhone 11 (FirstNet)	7/9/2020	11/19/2020	11/19/2020	Forever	5
iPhone 11 (FirstNet)	7/9/2020	11/19/2020	7/8/2020	Forever	5

**Figure 5. Durkan’s text message retention settings**

#### Communication Applications (former Mayor Durkan)

The standard iPhone Mail, iMessage, and Phone applications were located on each of the backups of Durkan’s iPhones.

The full file system extraction from Durkan's iPhone 11 (FirstNet) contained a database of Microsoft Teams messages. The **ZSMESSAGE** table found in the **SkypeSpacesDogfood-78e61e45-6beb-4009-8f99-359d8b54f41b.sqlite** database contained 1,799 entries. An analysis of the Teams content showed that the database contained 653 messages and 490 "Event/Call" records dated between April 15, 2020, and November 17, 2020.

I did not find evidence of other communication applications having been downloaded, installed, or used on the backups and forensic extractions provided for Durkan.

#### **Factory Reset (former Mayor Durkan)**

On July 4, 2020, Durkan's iPhone 8 Plus (FirstNet) was restored from an iCloud backup of itself. See Faulkner, 27-28. According to Apple<sup>6</sup>, in order to restore from an iCloud backup, the iPhone must first be erased, or factory reset, indicating that the iPhone 8 Plus (FirstNet) must have been factory reset on July 4, 2020.

On September 17, 2020, Durkan's iPhone 8 Plus (FirstNet) was factory reset a second time. This is evidenced by examining the full file system extraction of Durkan's iPhone 8 Plus (FirstNet) that was created on July 7, 2021. As discussed in the "Evidence of Devices Having Been Factory Reset" section above, certain forensic artifacts provide information about when an iPhone was factory reset. The July 7, 2021, backup of Durkan's iPhone 8 Plus (FirstNet) contained an **.obliterated** file that was created on September 17, 2020, at 6:56pm PDT. This special 0 byte file was found in the **/private/var/root/** folder and provides an indication of when the device was factory reset. The **containermanagerd.log.0**<sup>7</sup> file also included an entry describing when the iPhone was started up and confirms that Durkan's iPhone 8 Plus (FirstNet) completed the factory reset process on September 17, 2020, at 6:56pm PDT.

#### **Evidence of Failed Credentials (former Mayor Durkan)**

On November 16, 2020, one of the City's forensic vendors attempted to collect text messages that were synchronized with and stored on Durkan's iCloud account. Text messages, among other data types, are stored on iCloud with end-to-end encryption<sup>8</sup>. In order to download the text messages from a user's iCloud account, the passcode for one of the user's connected devices must first be entered. According to the City's November 1, 2021, ESI Log, the end-to-end encrypted or "protected data", including Durkan's text messages, was not downloaded "due to authentication issues". The City did not successfully collect text messages from Durkan's iCloud account until September 9, 2021.

#### **Evidence of File Deletion (former Mayor Durkan)**

When Durkan's iPhone 8 Plus (FirstNet) was factory reset and subsequently restored from an iCloud backup on July 4, 2020, approximately 5,911 messages were restored from her iCloud account. After the messages were restored to her iPhone 8 Plus (FirstNet), the "Messages in iCloud" feature was turned off and the "Disable & Delete" option was selected on July 4, 2020, at 5:19pm PDT. See Faulkner,

---

<sup>6</sup> See "Restore your device from an iCloud backup", <https://support.apple.com/en-us/HT204184>

<sup>7</sup> The "containermanagerd.log.0" is located at **/private/var/root/Library/Logs/MobileContainerManager** and is typically only found in full filesystem extractions.

<sup>8</sup> See <https://support.apple.com/en-us/HT202303> for information regarding the end-to-end encryption used by Apple's iCloud service.



28-29. This action resulted in nearly 6,000 text messages being deleted from Durkan's iCloud account 30 days later, on August 4, 2020. *Id.*

Sometime between July 4, 2020, and July 26, 2020, Durkan's iPhone was configured to delete all text messages older than 30 days. See Faulkner, 33-34. The City's expert provides a detailed description of how text messages are sequentially numbered using the **ROWID** field found in **message** and **chat** tables in the iPhone's **sms.db** text message database. *Id.*, 28-29. An assessment of the text message database from Durkan's iPhone 11 (FirstNet) indicates that the first and newest message that was downloaded from iCloud after the phone had been factory reset was dated July 4, 2020, at 11:44am PDT, and was assigned **ROWID** 1. The oldest remaining message was dated June 25, 2020, at 10:38am PDT and assigned **ROWID** 165. The first remaining message that was received after Durkan's phone was restored was dated July 4, 2020, at 8:18pm PDT and assigned **ROWID** 5,912. All messages between **ROWID** 165 and 5,912 are missing, indicating that the 30-day retention setting deleted 5,746 messages that were dated prior to June 25, 2020, at 10:38am PDT.

In addition to the 30-day retention setting which automatically deleted messages, I found evidence that messages were manually deleted as well. The City's expert concluded that the 30-day retention setting was turned off on approximately July 25, 2020. See Faulkner, 33-34. As a result, the only messages deleted by the 30-day retention setting would have been dated prior to June 25, 2020, at 10:38am PDT, the oldest remaining message. Since messages received on an iPhone are added to the **sms.db** text message database sequentially, one can look for gaps in the message table's **ROWID** to identify manually deleted messages. An assessment of the text message database found in the July 8, 2021, collection of Durkan's iPhone 11 (FirstNet) includes gaps in the **message** table **ROWIDs**, indicating that messages were manually deleted. The missing messages may have been deleted individually, one message at a time, or may have been the result of entire conversation threads having been deleted by a single action. My analysis of the **ROWID** gaps in the **message** table shows that an additional 191 messages were manually deleted between June 25, 2020, and November 16, 2020. Adding the 191 manually deleted messages to the 5,746 messages deleted by the 30-day retention setting yields 5,937 messages that were deleted after the iPhone 8 Plus (FirstNet) was factory reset on July 4, 2020. This is confirmed by the **sqlite\_sequence** table in the **sms.db** text message database found on the July 8, 2021, collection of Durkan's iPhone 11 (FirstNet). In this table, both the **sync\_deleted\_messages** and **deleted\_messages** values were set to 5,937. A table detailing the number of deleted messages, the date range for which each of the missing messages was sent or received, and the method of deletion is provided as Exhibit C to this report.

The table below summarizes the contents of the **message** table found in the **sms.db** text message database for each of the collections of Durkan's iPhones. "Total Messages" is the maximum **ROWID** and reflects the number of messages sent or received. "Messages Remaining" is a count of the messages remaining in the **message** table. "Deleted Messages" is calculated by subtracting the number of "Messages Remaining" from the "Total Messages". "Deleted Messages as % of Total" is calculated by dividing the number of "Deleted Messages" by the number of "Total Messages". See figure 6.

Phone	Backup Date	Total Messages	Messages Remaining	Deleted Messages	Deleted Messages as % of Total
iPhone 8 Plus (Verizon)	8/29/2019	4,722	3,643	1,079	22.9%
iPhone 8 Plus (Verizon)	7/2/2021	4,938	3,845	1,093	22.1%
iPhone 11 (FirstNet)	8/21/2020	6,875	1,006	5,869	85.4%
iPhone 11 (FirstNet)	10/15/2020	7,635	1,702	5,933	77.7%
iPhone 11 (FirstNet)	11/19/2020	8,162	2,225	5,937	72.7%
iPhone 11 (FirstNet)	7/8/2021	8,162	2,225	5,937	72.7%

**Figure 6. Evaluation of messages deleted from Durkan’s iPhones**

While I cannot determine the exact date that each message was deleted, I can compare the **sms.db** text message databases from each successive backup of Durkan’s iPhone 11 (FirstNet) and determine that 64 messages were deleted between August 21, 2020, and October 15, 2020, and another 4 messages between October 15, 2020, and November 19, 2020. In total, 191 text messages were manually deleted from Durkan’s iPhone between July 4, 2020, and November 19, 2020.

#### **Evidence of Data Wiping and Hiding (former Mayor Durkan)**

See “Evidence of File Deletion” section above.

#### **Evidence of ESI Available from Other Sources (former Mayor Durkan)**

I did not identify any additional sources of data likely to contain Durkan’s missing text messages that had not been collected and identified on the ESI Log provided by the City.

#### **Assessment of Forensic Extractions and Backups (former Mayor Durkan)**

The forensic extractions and backups provided for Durkan’s iPhones and iCloud account were consistent with what I would expect to obtain; however, had data been collected from Durkan’s iCloud account prior to it expiring, the City should have been able to recover most of the 5,937 deleted text messages.

## 13.2 Former Chief Best

#### **Text Message Retention Settings (former Chief Best)**

The City provided one backup of Best’s iPhone XS Max that she used between October 1, 2019, and September 2, 2020. When the backup was created on February 24, 2021, the phone was configured to delete all messages older than 30 days. The following table provides additional detail about the text message retention settings found on Best’s iPhone. See figure 7.



Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone XS Max	10/1/2019	9/2/2020	2/24/2021	30	2

Figure 7. Best's text message retention settings

#### Communication Applications (former Chief Best)

In addition to the default iPhone Mail, iMessage, and Phone applications, the Microsoft Teams, Twitter, Facebook, and LinkedIn applications were also installed on Best's iPhone XS Max. However, I did not locate recoverable messages or other forms of communication sent or received by these applications.

#### Evidence of Devices Having Been Factory Reset (former Chief Best)

Best's iPhone XS Max was first set up by transferring data from her prior iPhone 8 Plus on October 1, 2019. *See* Faulkner, 37-38. I did not find evidence that her iPhone XS Max had been factory reset since it was first used on October 1, 2019.

#### Evidence of Failed Credentials (former Chief Best)

I did not find evidence that failed credentials impacted the City's ability to access or collect information from Best's iPhone XS Max.

#### Evidence of File Deletion (former Chief Best)

The February 24, 2021, collection of Best's iPhone XS Max only included 15 text messages, all of which were received on September 2, 2020, the last day the phone was used. In addition to the 15 remaining messages, there were another 49 entries related to group chats found in the **message** table of the **sms.db** text message database. *See* Faulkner, 41. None of the 49 entries included message text. The maximum **ROWID** for the **message** table was 27,202, and subtracting the 15 messages and 49 chat entries from the maximum **ROWID** indicates that 27,138 messages had been deleted from Best's iPhone XS Max. The number of deleted messages is confirmed by an entry in the **sqlite\_sequence** table where the **deleted\_messages** value was also set to 27,138.

It appears that nearly all the 27,138 messages deleted from Best's iPhone XS Max were deleted manually, as opposed to having been automatically deleted by the configured 30-day message retention setting. Only 28 out of 5,133 entries remain in the **chat** table, indicating that messages associated with the 5,105 missing chat entries were deleted manually.

The following table summarizes the contents of the **message** table found in the **sms.db** text message database from the collection of Best's iPhone XS Max. "Total Messages" is the maximum **ROWID** and reflects the number of messages sent or received. "Messages Remaining" is a count of the messages remaining in the **message** table. "Deleted Messages" is calculated by subtracting the number of "Messages Remaining" from the "Total Messages". "Deleted Messages as % of Total" is calculated by dividing the number of "Deleted Messages" by the number of "Total Messages". *See* figure 8.

Phone	Backup Date	Total Messages	Messages Remaining <sup>9</sup>	Deleted Messages	Deleted Messages as % of Total
iPhone XS Max	2/24/2021	27,202	64	27,138	99.8%

**Figure 8. Evaluation of messages deleted from Best's iPhone XS Max**

#### **Evidence of Data Wiping and Hiding (former Chief Best)**

See "Evidence of File Deletion" section above.

#### **Evidence of ESI Available from Other Sources (former Chief Best)**

An inspection of the **com.apple.mobile.ldbbackup.plist** file shows that the last iCloud backup was completed on October 1, 2019, and that the phone had not been backed up to iTunes. The October 1, 2019, backup would have expired and been automatically deleted from her iCloud account after 180 days.

I did not identify any additional sources of data likely to contain Best's missing text messages that had not been collected and identified on the ESI Log provided by the City.

#### **Assessment of Forensic Extractions and Backups (former Chief Best)**

The forensic extractions and backups provided for Best's iPhones and iCloud account were consistent with what I would expect to obtain.

### 13.3 Chris Fisher

#### **Text Message Retention Settings (Chris Fisher)**

The City provided one backup of Fisher's iPhone 7 that he used between October 1, 2019, and September 2, 2020. When the backup was created on February 22, 2021, the phone was configured to delete all messages older than 30 days. The following table provides additional detail about the text message retention settings found on Fisher's iPhone. See figure 9.

Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone 7	11/2/2020 <sup>10</sup>	12/9/2020	2/22/2021	30	1

**Figure 9. Fisher's text message retention settings**

<sup>9</sup> The **sms.db - message** table has 64 entries remaining, however only 16 were actual text messages and contained content.

<sup>10</sup> Fisher's iPhone 7 appears to have been restored from an iCloud backup on 11/2/2020 at 4:52PM PST. See "Factory Reset" section below for more detail.

### Communication Applications (Chris Fisher)

In addition to the default iPhone Mail, iMessage, and Phone applications, Microsoft Teams was also installed on Fisher's iPhone 7; however, I did not locate recoverable messages or other forms of communication sent or received by the Microsoft Teams application.

### Evidence of Devices Having Been Factory Reset (Chris Fisher)

The **com.apple.MobileBackup.plist** configuration file contained a **RestoreDate** key set to "11/3/2020 12:52:14 AM" and the **WasCloudRestored** key set to "True". This combination of values indicates that Fisher's iPhone 7 was restored from an iCloud backup on November 2, 2020, at 4:52PM PST. To restore an iPhone from an iCloud backup, it would first need to be erased or "factory reset".<sup>11</sup>

### Evidence of Failed Credentials (Chris Fisher)

The City reported that on approximately December 3, 2020, Fisher experienced an issue with the facial recognition functionality on his iPhone 7, and that he did not remember his passcode<sup>12</sup>. This resulted in Fisher becoming locked out of his iPhone 7, and ultimately it was factory reset.

The iPhone 7 does not support facial recognition, or more specifically, "Face ID". Either the explanation was incorrect, or the incident that Fisher described was with a different phone. As described in the "Evidence of ESI Available from Other Sources" section below, Fisher appears to have used an iPhone XS and iPhone 12 Pro, both of which support apple Face ID. However, no data was provided from either of these phones.

### Evidence of File Deletion (Chris Fisher)

The February 22, 2021, collection of Fisher's iPhone 7 only included 16 text messages, all of which were received between December 3, 2020, and December 8, 2020. The maximum **ROWID** for the **message** table was 15,859 and subtracting the 16 messages indicates that 15,843 messages had been deleted from Fisher's iPhone 7. The number of deleted messages is confirmed by an entry in the **sqlite\_sequence** table where the **deleted\_messages** value was also set to 15,843.

The following table summarizes the contents of the **message** table found in the **sms.db** text message database for Fisher's iPhone 7. "Total Messages" is the maximum **ROWID** and reflects the number of messages sent or received. "Messages Remaining" is a count of the messages remaining in the **message** table. "Deleted Messages" is calculated by subtracting the number of "Messages Remaining" from the "Total Messages". "Deleted Messages as % of Total" is calculated by dividing the number of "Deleted Messages" by the number of "Total Messages". See figure 10.

<sup>11</sup> See "Restore your device from an iCloud backup", <https://support.apple.com/en-us/HT204184>

<sup>12</sup> See City's Aug. 31, 2021, Supplemental Response to Plaintiffs' Second Set of Interrogatories to Defendant City of Seattle.

Phone	Backup Date	Total Messages	Messages Remaining	Deleted Messages	Deleted Messages as % of Total
iPhone 7	2/22/2021	15,859	16	15,843	99.9%

**Figure 10. Evaluation of messages deleted from Fisher’s iPhone 7**

### Evidence of Data Wiping and Hiding (Chris Fisher)

See “Evidence of File Deletion” section above.

### Evidence of ESI Available from Other Sources (Chris Fisher)

The iPhone 7 backup provided for Fisher included photos that were restored from his iCloud account. Within the individual photos is metadata, or information that describes when the original photo was taken, the model of camera used to take the photo, as well as other details about the photo. Of the photos restored from Fisher’s iCloud account, 2,955 were taken with three different models of iPhones between October 10, 2016, and December 6, 2020<sup>13</sup>. See figure 11.

iPhone Model	First Photo	Last Photo	Count of Photos
iPhone 7 Plus	10/10/2016	9/21/2018	1,187
iPhone XS	9/22/2018	10/23/2020	1,720
iPhone 12 Pro	10/31/2020	12/6/2020	48

**Figure 11. iPhone models used to take photos restored from Fisher’s iCloud account**

This metadata shows that Fisher likely used an iPhone XS between September 22, 2018, and October 23, 2020, and switched to an iPhone 12 Pro after that. Additionally, the iPhone used to take the photos between October 10, 2016, and September 21, 2018, is listed as an “iPhone 7 Plus”, not the “iPhone 7” that was the source of the February 22, 2021, backup provided by the City.

A review of the text messages produced by the City for former Mayor Durkan and former Chief Best include text messages that were sent to Fisher using the **Redacted** phone number; however, when Fisher’s iPhone 7 was backed up on February 22, 2021, the last phone number used by the phone was **Redacted**. The **CellularUsage.db** shows that the **subscriber\_mdn** was set to **Redacted**. The **chat** table in the **sms.db** text message database shows that the “account\_login” for the iPhone 7 was set to “P:+12067754995” and “E:**Redacted**”. However, the “last\_addressed\_handle” in the **chat** table shows that both the **Redacted** and **+Redacted** phone numbers were used over time. There are a variety of possible explanations for this scenario, such as switching the SIM card used in the phone; however, it appears that Fisher may have sources of text messages that were not collected.

<sup>13</sup> Fisher’s iCloud Photos backup include another 76 photos that were taken with several other iPhone models; however, these were likely received from another user via text message, email, or another transfer method and saved to his device.

Based on my review of the evidence provided, it appears that Fisher used an iPhone XS and iPhone 12 Pro during the relevant time period. Data from the iPhone XS and iPhone 12 Pro was not provided and is a likely source of relevant information.

#### Assessment of Forensic Extractions and Backups (Chris Fisher)

Fisher's iPhone 7 was backed up by the City's vendor on February 22, 2021. At that time, the last successful iCloud backup for the iPhone 7 was on December 2, 2020.<sup>14</sup> This backup, and one from the prior week, should still have been available at the time the phone was collected on February 22, 2021. Since the phone was not configured to synchronize messages with iCloud<sup>15</sup>, any messages remaining on the phone as of December 2, 2020, would have been stored in the iCloud backup. However, since more than 180 days has elapsed, it is likely that the iCloud backup for this phone has expired and is no longer available on Fisher's iCloud account.

### 13.4 Kenneth Neafcy

#### Text Message Retention Settings (Kenneth Neafcy)

The City provided backups of two different iPhones used by Neafcy, an iPhone 6s and an iPhone XS. The phone that Neafcy used between approximately March 20, 2020, and October 27, 2020, was factory reset, and thus the text message retention settings configured for this phone are not known. Neafcy began using an iPhone 6s after the iPhone XS was reset, and the iPhone 6s was configured to retain text messages forever. The following table provides additional detail about the text message retention settings found on each of Neafcy's iPhones. See figure 12.

Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone XS	Approx. 3/20/2020	10/27/2020 <sup>16</sup>	8/17/2021	Unknown, Phone was factory reset	
iPhone 6s <sup>17</sup>	10/29/2020	3/1/2021	3/1/2021	Forever	0
iPhone 6s	10/29/2020	3/9/2021	10/27/2021	Forever	0
iPhone 6s	10/29/2020	3/9/2021	10/30/2021	Forever	0

Figure 12. Neafcy's text message retention settings

<sup>14</sup> The **LastCloudBackupDate** key from the **com.apple.lidbackup.plist** configuration file shows that the last successful iCloud backup was at 2020-12-02 21:20:17 UTC.

<sup>15</sup> The **CloudKitSyncingEnabled** key from the **com.apple.madrid.plist** configuration file was set to "False", indicating that the messages in iCloud feature was not used.

<sup>16</sup> Neafcy's iPhone XS appears to have been factory reset on 10/27/2020 at approximately 10:26pm. It is unclear when he started to use the iPhone XS; however, it is likely that he began using it on approximately 3/20/2020, after he stopped using his iPhone 6s. See the "Factory Reset" section below for additional detail.

<sup>17</sup> Neafcy used the iPhone 6s from 10/29/2020 – 3/9/2021, after his iPhone XS was factory reset. It appears that he had used the same iPhone 6s between 6/15/2017 - 3/20/2020, prior to his use of the iPhone XS.

### Communication Applications (Kenneth Neafcy)

In addition to the default iPhone Mail, iMessage, and Phone applications, the Microsoft Teams and Facebook applications were also installed on Neafcy's iPhone 6s. However, I did not locate recoverable messages or other forms of communication sent or received by the Microsoft Teams or Facebook applications.

### Evidence of Devices Having Been Factory Reset (Kenneth Neafcy)

The City reported that Neafcy became locked out of his iPhone XS and ultimately, it was factory reset. An inspection of the databases and log files found on the August 17, 2021, backup of his iPhone XS shows that the factory reset likely occurred on October 27, 2020, at 3:26pm PT. The first entries in the **ZPROCESS** and **ZLIVEUSAGE** tables from the **DataUsage.sqlite** database reflect this time, as do the creation times for the **sms.db**, **Accounts3.sqlite**, and other system databases that are typically created when a phone first boots after a factory reset.

### Evidence of Failed Credentials (Kenneth Neafcy)

The City reported that Neafcy became locked out of his iPhone XS and ultimately, it was factory reset.

### Evidence of File Deletion (Kenneth Neafcy)

Neafcy's iPhone XS was factory reset on October 27, 2020, resulting in the loss of all text messages that he sent or received between March 19, 2020, and October 28, 2020<sup>18</sup>. Since the phone was factory reset, I am not able to inspect the **sms.db** text message database and determine how many messages were lost.

The following table summarizes the contents of the **message** table found in the **sms.db** text message database for the two collections of Neafcy iPhone 6s. "Total Messages" is the maximum **ROWID** and reflects the number of messages sent or received. "Messages Remaining" is a count of the messages remaining in the **message** table. "Deleted Messages" is calculated by subtracting the number of "Messages Remaining" from the "Total Messages". "Deleted Messages as % of Total" is calculated by dividing the number of "Deleted Messages" by the number of "Total Messages". See figure 13.

Phone	Backup Date	Total Messages	Messages Remaining	Deleted Messages	Deleted Messages as % of Total
iPhone 6s	10/27/2021	2,540	2,498	42	1.7%
iPhone 6s	3/1/2021	2,472	2,430	42	1.7%

**Figure 13. Evaluation of messages deleted from Neafcy's iPhone 6s**

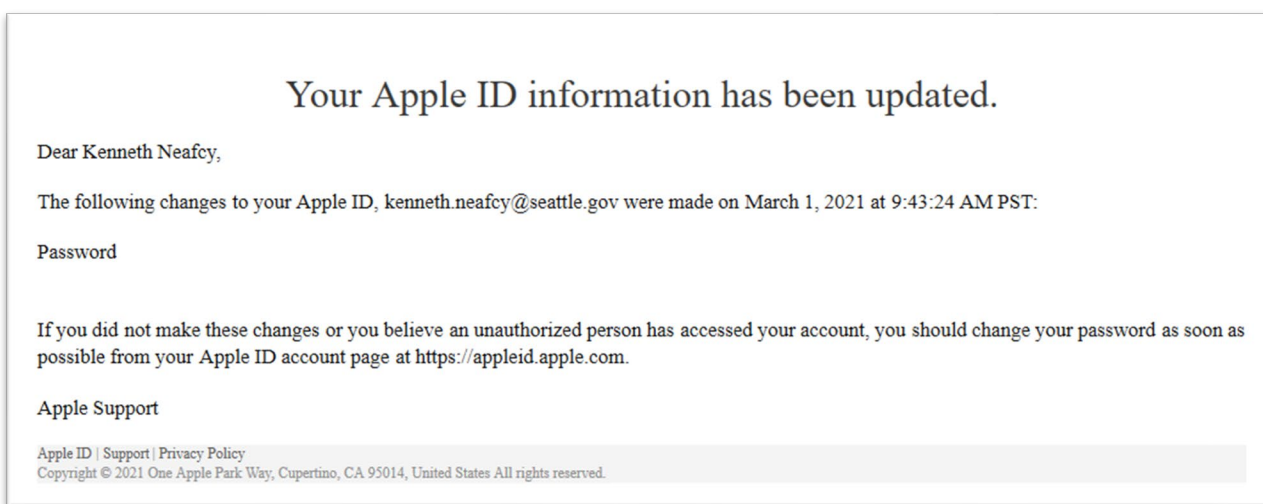
<sup>18</sup> An inspection of the message table from the sms.db backed up from Neafcy's iPhone 6s on March 1, 2021, shows a gap of messages between March 19, 2020, at 5:28pm PDT, and October 28, 2020, at 2:37pm PDT.

### Evidence of Data Wiping and Hiding (Ken Neafcy)

See “Evidence of File Deletion” section above.

### Evidence of ESI Available from Other Sources (Ken Neafcy)

The City reported that Neafcy “tried to recover the phone from iCloud, but it sent the passcode to the phone that was locked so he could not view it.”<sup>19</sup> An inspection of Neafcy’s iPhone 6s shows that his iCloud account was associated with his **Redacted** email address<sup>20</sup>. The October 27, 2021, backup of his iPhone 6s included two emails from Apple Support. The first message reported that the password associated with his iCloud account was changed on March 1, 2021, and the second reported that an iPhone XR was used to sign into his iCloud account on March 6, 2021. See Figures 14 and 15.

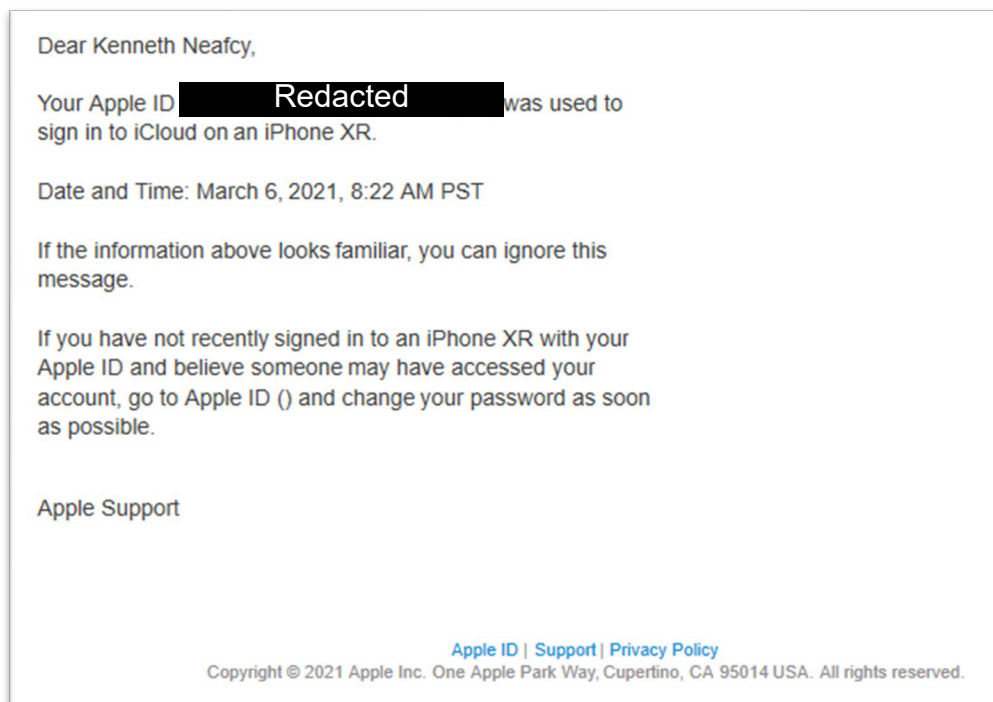


**Figure 14. March 1, 2021, email from Apple Support reporting that the password for Neafcy’s **Redacted** iCloud account was changed**

<sup>19</sup> See City’s Aug. 31, 2021, Supplemental Response to Plaintiffs’ Second Set of Interrogatories to Defendant City of Seattle.

<sup>20</sup> The **ZUSERNAME** field in the **Accoutns3.sqlite** database found on the backups of Neafcy’s iPhone 6s was set to **Redacted** for various Apple services, indicating this was the currently configured Apple ID.





**Figure 15. March 6, 2021, email from Apple Support reporting that Neafcy signed into his iCloud account with an iPhone XR**

It is unclear how long Neafcy lost access to his iCloud account; however, if his iPhone XS was backed up to his iCloud account before it was factory reset on October 27, 2020, that backup would have been kept for 180 days and would still have been available when data was collected from his iPhone 6s on March 1, 2021.

#### **Assessment of Forensic Extractions and Backups (Ken Neafcy)**

See “Evidence of ESI Available from Other Sources” section above.

### 13.5 Chief Scoggins

#### **Text Message Retention Settings (Chief Scoggins)**

The City provided backups of two different iPhones used by Chief Scoggins. Chief Scoggins’ iPhone 8 Plus was factory reset on October 8, 2020, and thus the text message retention settings prior to the reset date are unknown. Between October 8, 2020, and February 16, 2021, the iPhone 8 Plus was configured to retain messages forever. On February 17, 2021, files and settings from Chief Scoggins iPhone 8 were transferred to a new iPhone 11<sup>21</sup>. The iPhone 11 was also configured to retain text

<sup>21</sup> The **com.apple.MobileBackup.plist** found on Scoggins’ iPhone 11 contained a **RestoreDate** key set to “2/18/2021 12:42:24 AM” UTC, a **WasCloudRestore** key set to “False”, and a **SourceDeviceUDID** key set to “6198ec80e016c39394d59e4687b191edc6112c1d”, which matches the unique id of Scoggins’ iPhone 8 Plus. This



messages “Forever” when it was last backed up on March 9, 2021. The following table provides additional detail about the text message retention settings found on each of Chief Scoggins’ iPhones. See figure 16.

Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone 8 Plus	10/8/2020	2/12/2021	2/13/2021	Forever	0
iPhone 8 Plus	10/8/2020	2/16/2021	2/16/2021	Forever	0
iPhone 11	2/17/2021	3/9/2021	3/9/2021	Forever	1

**Figure 16. Chief Scoggins’ text message retention settings**

### Communication Applications (Chief Scoggins)

In addition to the default iPhone Mail, iMessage, and Phone applications, the Microsoft Teams and Twitter applications were also installed on Scoggins’ iPhone 8 Plus and iPhone 11. However, I did not locate recoverable messages or other forms of communication sent or received by these applications.

### Evidence of Devices Having Been Factory Reset (Chief Scoggins)

The City reported that Chief Scoggins became locked out of his iPhone 8 Plus on October 8, 2020, and as a result, his phone was factory reset. An inspection of the February 16, 2021, iPhone 8 Plus iCloud backup provided by the City confirms that the phone had been factory reset and the first subsequent use began on October 8, 2020. The first entries in the **ZPROCESS** and **ZLIVEUSAGE** tables from the **DataUsage.sqlite** database are October 8, 2020, at 4:15pm PDT and 4:16pm PDT respectively. The first messages were found in the **sms.db** text message database just over an hour later at 5:22pm PDT on October 8, 2020.

### Evidence of Failed Credentials (Chief Scoggins)

The City reported that Chief Scoggins had forgotten his iPhone passcode and became locked out his iPhone 8 Plus on October 8, 2020, and the phone was subsequently factory reset.

### Evidence of File Deletion (Chief Scoggins)

Chief Scoggins iPhone 8 Plus was factory rest on October 8, 2020, resulting in the loss of all text messages prior to that date.

The following table summarizes the contents of the **message** table found in the **sms.db** text message database from the collections of Scoggins’ iPhone 8 Plus and iPhone 11. “Total Messages” is the maximum **ROWID** and reflects the number of messages sent or received. “Messages Remaining” is a count of the number of messages remaining in the **message** table. “Deleted Messages” is calculated by subtracting the number of “Messages Remaining” from the “Total Messages”. “Deleted Messages as % of Total” is calculated by dividing the number of “Deleted Messages” by the number of “Total Messages”. See figure 17.

---

combination of keys indicates that Scoggins’ iPhone 8 Plus was transferred to his new iPhone 11 on February 17, 2021, at 4:42pm PST.

Phone	Backup Date	Total Messages	Messages Remaining	Deleted Messages	Deleted Messages as % of Total
iPhone 8 Plus	2/13/2021	2,829	2,827	2	0.1%
iPhone 8 Plus	2/16/2021	2,948	2,946	2	0.1%
iPhone 11	3/9/2021	3,335	3,333	2	0.1%

**Figure 17. Evaluation of messages deleted from Scoggins' iPhones**

#### **Evidence of Data Wiping and Hiding (Chief Scoggins)**

See "Evidence of File Deletion" section above.

#### **Evidence of ESI Available from Other Sources (Chief Scoggins)**

Chief Scoggins iPhone 8 Plus and iPhone 11 were both configured to backup to his iCloud account and the City provided two restored iCloud backups for his iPhone 8 Plus. Included with the backups was a configuration file named [REDACTED] **Redacted** that was created by the forensic software used to download the backups. The "last\_snapshot\_date" values for the iPhone 8 Plus were February 13, 2021, at 1:19:44, and February 16, 2021, at 22:07:40. The **com.apple.mobile.ldbbackup.plist** found in the backup of his iPhone 11 had the key **LastCloudBackupDate** set to "2021-03-09 05:57:46.0000000 Z"<sup>22</sup> and the key **CloudBackupEnabled** set to "True". Had Chief Scoggins iPhone 8 Plus been configured to backup to iCloud at the time it was factory reset on October 8, 2020, the same process could have been used to download the backup from his iCloud account. However, since the same iPhone 8 Plus was configured to backup to the same iCloud account after it was factory reset, it is likely that the iCloud backups of the newly configured phone would have overwritten any existing backups within a few weeks.

#### **Assessment of Forensic Extractions and Backups (Chief Scoggins)**

The City's forensic vendor did not collect data from Chief Scoggins' iCloud account until July 15, 2021. At this time, his iCloud account had two backups for his iPhone 8 Plus, one from February 13, 2021, and the other from February 16, 2021. Had the City collected data from Chief Scoggins' iCloud account shortly after his iPhone 8 Plus was factory reset on October 8, 2020, the messages lost due to the factory reset may have been recovered.

## 13.6 Idris Beauregard

#### **Text Message Retention Settings (Idris Beauregard)**

The City provided one backup of the iPhone 8 used by Idris Beauregard. Beauregard's iPhone 8 was factory reset on October 9, 2020, and thus the text message retention settings prior to the reset event are unknown. An inspection of the **com.apple.MobileSMS.plist** file found on the March 9, 2021 backup

<sup>22</sup> Dates can be stored in many different formats. The **LastCloudBackup** key is stored in Apple Absolute Time, which is the number of seconds that have elapsed since "2001-01-01 00:00:00 Z". This numeric value can be converted to a human readable date using a specific formula.

of Beauregard's iPhone 8 did not contain entries for the **KeepMessageForDays** and **KeepMessagesVersionID** keys. This is consistent with the iPhone 8 having the default text message retention setting of "Forever". See figure 18.

Device	Use Date (Start)	Use Date (End)	Backup Date	Message Retention Setting	Message Retention Version
iPhone 8	10/9/2020	3/9/2021	3/9/2021	Forever	0

**Figure 18. Beauregard's text message retention settings**

#### **Communication Applications (Idris Beauregard)**

In addition to the default iPhone Mail, iMessage, and Phone applications, the Microsoft Teams application was also installed on Beauregard's iPhone 8. However, I did not locate recoverable messages or other forms of communication sent or received by the Microsoft Teams application.

#### **Evidence of Devices Having Been Factory Reset (Idris Beauregard)**

The City reported that Beauregard had forgotten his iPhone 8 passcode and became locked out on October 9, 2020, and the phone was subsequently factory reset. An inspection of the **com.apple.purplebuddy.plist** configuration file shows that the "GuestCountry" - "at" key was set to October 9, 2020, at 1:51pm PDT and the "SetupLastExit" key was set to October 9, 2020 at 2:17pm PDT. The oldest entry in the **ZPROCESS** table found in the **DateUsage.sqlite** database was set to October 9, 2020, at 1:50pm PDT. These artifacts are consistent with the factory reset process completing at approximately 1:50pm PDT on October 9, 2020.

#### **Evidence of Failed Credentials (Idris Beauregard)**

The City reported that Beauregard had forgotten his iPhone 8 passcode and became locked out on October 9, 2020, and the phone was subsequently factory reset.

#### **Evidence of File Deletion (Idris Beauregard)**

Beauregard's iPhone 8 was factory reset on October 9, 2020, resulting in the loss of all text messages prior to that date. The **sms.db** text message database from Beauregard's iPhone 8 included 3,682 text messages that were sent and received between October 9, 2020, and March 9, 2021. Of the 3,682 messages, 388 messages were manually deleted from the phone. The maximum **ROWID** for the **message** table was 3,682, and subtracting the 3,294 remaining messages from the maximum **ROWID** indicates that 388 messages had been deleted from Beauregard's iPhone 8. This is confirmed by the **deleted\_messages** and **sync\_deleted\_messages** values from the **sqlite\_sequence** table, both of which were set to 388. Since Beauregard's iPhone 8 was configured to keep messages "Forever", the deletions must have been performed manually.

The following table summarizes the contents of the **message** table found in the **sms.db** text message database collected from Beauregard's iPhone 8. "Total Messages" is the maximum **ROWID** and reflects the number of messages sent or received. "Messages Remaining" is a count of the messages remaining in the **message** table. "Deleted Messages" is calculated by subtracting the number of "Messages

Remaining” from the “Total Messages”. “Deleted Messages as % of Total” is calculated by dividing the number of “Deleted Messages” by the number of “Total Messages”. See figure 19.

Phone	Backup Date	Total Messages	Messages Remaining	Deleted Messages	Deleted Messages as % of Total
iPhone 8	3/9/2021	3,682	3,294	388	10.5%

**Figure 19. Evaluation of messages deleted from Beauregard’s iPhones**

#### **Evidence of Data Wiping and Hiding (Idris Beauregard)**

See “Evidence of File Deletion” section above.

#### **Evidence of ESI Available from Other Sources (Idris Beauregard)**

Since Beauregard’s iPhone 8 was factory reset, I am not able to determine if his phone had been backed up using iTunes or iCloud before it was reset on October 9, 2020. However, when his iPhone 8 was collected on March 9, 2021, the **com.apple.mobile.lidbackup.plist** configuration file had the **CloudBackupEnabled** key set to “True”, indicating that it was configured to backup to iCloud.<sup>23</sup> If his phone was backed up to iCloud prior to October 9, 2020, the backup would only have been available for 180 days and would have expired by approximately April 7, 2021.

#### **Assessment of Forensic Extractions and Backups (Idris Beauregard)**

See “Evidence of ESI Available from Other Sources” section above.

### 13.7 Assistant Chief Greening

The City provided three backups of Greening’s Samsung Galaxy S8 phone. Greening was the only one of the City Officials subject to the October 29, 2021 Digital Examination Agreement and Order that used an Android device. The process to extract information from an Android device is different than that of an iPhone, as are the forensic artifacts used to determine the configuration of the phone and past activity. The provided forensic extractions were limited, and while the content of the available text messages was included, the **mmssms.db** text message database and other configuration files were not. This is consistent with the capabilities of a standard forensic extraction. Extracting additional data from the phone, including the **mmssms.db** text message database, would have required “rooting” the phone to bypass the device security or using specialized software or tools only available in some forensic labs.

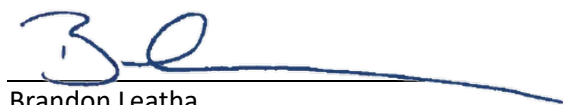
The City reported that Greening became locked out of his Samsung Galaxy S8 on October 26, 2020, and as a result, the phone was factory reset. An analysis of the available data shows that the oldest text

<sup>23</sup> The **com.apple.mobile.lidbackup.plist** configuration file had the **CloudBackupEnabled** key set to “True”. The **LastCloudBackupDate** did not exist, indicating that an iCloud backup had not yet been completed. This may be because the iCloud backup setting was enabled shortly before data was extracted from his phone on March 9, 2021, or because he did not have enough available storage in his iCloud account.

message was dated October 27, 2020, at 8:28AM PDT, and the oldest call record was dated October 26, 2020, at 12:43pm PDT. The oldest files, including the **SamsungAnalyticsPrefs.xml** configuration file, were dated October 26, 2020, at 9:14AM PDT. This is consistent with the phone having been factory reset on the morning of October 26, 2020, prior to 9:14AM PDT.

---

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "BL", with a long horizontal flourish extending to the right.

Brandon Leatha

April 28, 2022

## Exhibit A – Materials Considered

- Documents Produced by the City of Seattle
  - BEST\_00000002 – Text messages between Carmen Best and Chris Fisher from May 18, 2021 to June 8, 2021
  - CONFIDENTIAL\_Durkan\_Jenny\_messages\_supplemental\_V2.xls (a partial reconstruction of Jenny Durkan’s text messages)
  - CONFIDENTIAL\_Durkan\_Jenny\_messages\_supplemental\_V3.xls (a partial reconstruction of Jenny Durkan’s text messages)
  - CONFIDENTIAL\_HC\_Durkan\_Jenny\_messages\_supplemental.xls (a partial reconstruction of Jenny Durkan’s text messages)
  - CONFIDENTIAL\_HC-Best\_Carmen\_messages\_supplemental.xls (a partial reconstruction of Carmen Best’s text messages)
  - CONFIDENTIAL\_Scoggins\_Harold\_messages 01.xls (a partial reconstruction of Harold Scoggins’s text messages)
  - CONFIDENTIAL\_Scoggins\_Harold\_messages 02.xls (a partial reconstruction of Harold Scoggins’s text messages)
  - CONFIDENTIAL\_Scoggins\_Harold\_messages 03.xls (a partial reconstruction of Harold Scoggins’s text messages)
  - SEA\_00144347 – March 4, 2021 Whistleblower Complaint by Stacy Irwin and supporting materials
  - SEA\_00145711 – Phone Log for Mayor Durkan’s work phone
- 2021-07-13 The City of Seattle’s Objections and Responses to the Plaintiffs’ Second Set of Interrogatories to Defendant City of Seattle
- 2021-08-03 Letter from Shane P. Cramer to Plaintiffs’ Counsel re Durkan Text Messages
- 2021-08-31 The City of Seattle’s Objections and Supplemental Responses to Plaintiff’s Second Set of Interrogatories to Defendant City of Seattle
- 2021-10-19 Stipulated Digital Examination Agreement (DEA) and Order Signed by Judge Zilly (Dkt. No. 50)
- 2021-11-01 ESI Log Produced Pursuant to the Stipulated Digital Examination Agreement
- 2022-02-11 Expert Report of Kevin T. Faulkner Dated February 11, 2022
- Deposition Transcript of Jenny A. Durkan Dated March 1, 2022, in the case of Seattle Times Co. v. City of Seattle, Case No. 21-2-07268-9 SEA, 92 - 105

## Exhibit B – Leatha CV



## Brandon Leatha

---

Founder and CEO, Leatha Consulting LLC

### SUMMARY

Brandon Leatha, the Founder and CEO of Leatha Consulting LLC, is an expert in digital forensics, e-Discovery, and data analytics. With over 22 years of technology consulting experience, he advises clients on digital forensic investigations, e-Discovery, information governance, and cybersecurity. Mr. Leatha has experience with on premise and cloud-based enterprise software platforms, such as email, database, and industry specific business applications. He has performed forensic investigations on hundreds of devices ranging from computers and enterprise servers, to smartphones and IOT devices. He has developed solutions to identify, preserve, and produce relevant information from a variety of challenging data sources, including social media, mobile applications, cloud-based applications, and legacy systems. He also has extensive experience designing and implementing data preservation plans, as well as assessing and remediating potential data loss situations.

Mr. Leatha has been a corporate 30(b)(6) witness, a court-appointed neutral computer forensics expert, and has testified on numerous electronic discovery and computer forensics issues. He has a certificate in computer forensics from the University of Washington and has earned both the GIAC Certified Incident Handler (GCIH) and GIAC Certified Forensic Examiner (GCFE) certificates. He serves on the Board of Directors for the Computer Technology Investigators Network (“CTIN”), is the Board Vice President of the Puget Sound chapter of the Information Systems Security Association (“ISSA”), and on the Advisory Board for the SANS Institute’s Global Information Assurance Certification (“GIAC”) program. He has been a member of the Sedona Conference since 2005 and has participated in the Working Groups on Electronic Document Retention and Production (“WG1”) and Data Security and Privacy Liability (“WG11”). Prior to his current role, he was a Director at Washington DC based iDiscovery Solutions (iDS) and the Director of ESI Consulting and Data Analysis at Electronic Evidence Discovery (EED).

### SELECT CONSULTING EXPERIENCE

- Managed the cross functional team that performed the data restoration, processing, analysis, hosted review, and production for one of the largest civil discovery disputes in history.
- Performed a covert collection and intellectual property theft investigation consisting of over 30 servers and workstations. Investigation resulted in the identification, quarantine, and secure deletion of the misappropriated intellectual property.
- Performed a forensic analysis of multiple computers and mobile devices to identify the installation and use of software that intercepted electronic communications.
- Performed the collection and production of relevant information originating from over 20 different social media accounts, many of which were not supported by industry standard forensic collection software and required the development, testing, and implementation of customized solutions.
- Responded to a targeted phishing attack which resulted in the compromise of multiple user credentials and significant financial loss. Led the incident response activities, including the planning, identification, containment, eradication, and remediation in a rapid and cost-effective manner.

## Exhibit B – Leatha CV



- Performed the collection, preservation, and production of incident information stored in legacy databases including DBII, Oracle, and SQL Server. Performed data conversion, normalization, and de-duplication to ensure the complete and non-duplicative production of relevant information. The resulting database allowed the client to quickly respond to discovery requests that were previously very costly and time consuming.
- For a public utility, performed an incident response investigation into the alleged theft and destruction of intellectual property which included the analysis of workstations, servers, security camera footage, and access control systems. Analysis required the correlation of evidence from multiple systems and locations over a multi-day period.
- Managed a team that collected, processed, and supported a multi-year hosted review of a significant volume of data onsite within an international corporation based in the EU.

## COURT APPOINTED NEUTRAL

- Court Appointed Neutral, Forensic Expert; TCS & Starquest Expeditions v. Distant Insights, PTC., LTD, Case No. 18-2-07338-3 SEA, Washington State Superior Court, King County; 2018-2021
- Court Appointed Neutral, Forensic Expert; Earthbound Corporation et al v. MiTek USA Inc et al, US District Court, Central District of California, Case No. 2:16-cv-07223-DMG-JPR; 2016-2017
- Court Appointed Neutral, Forensic Expert; Roger M. Belanich et al. v. Employers' Fire Insurance Co. et al., Superior Court of Washington for King County, Case No. 12-2-14368-4 SEA; 2014-2015

## TESTIMONY

- Expert report; Masood Khan v. The Greenspan Company, et al., Case No. 1100110442, Judicial Arbitration and Mediation Services, San Francisco Office; April 2022
- Expert report; Douglas Withers v. Boeing Employees' Credit Union, et al., Case No. 21-2-11224-9, Washington State Superior Court, King County; February 2022
- 30(b)(6) Deposition; St. Clair County Employees' Retirement System v. Acadia Healthcare Company, Inc. et al., Case No. 3:18-cv-00988, United States District Court for Middle District of Tennessee, Nashville Division; December 2021
- Declaration; City of Chicago v. Purdue Pharma L.P., et al., Case No. 14-CV-04261, United States District Court for the Northern District of Illinois, Eastern Division; July 2021
- Declaration; Pinkstaff v. Tidewater Barge Lines, Inc., Case No. 19-CV-54217, Oregon State Circuit Court, Multnomah County; May 2021
- Declaration; Pinkstaff v. Tidewater Barge Lines, Inc., Case No. 19-CV-54217, Oregon State Circuit Court, Multnomah County; May 2021
- Expert witness testimony, jury trial; John E. Traster v. NUGS LLC, Case No. 18-2-13981-3, Washington State Superior Court, King County; March 2021
- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; January 2021
- Declaration; John E. Traster v. NUGS LLC, Case No. 18-2-13981-3, Washington State Superior Court, King County; December 2020
- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; December 2020
- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; November 2020



Exhibit B – Leatha CV



- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; October 2020
- Expert witness testimony, evidentiary hearing; Masood Khan v. The Greenspan Company, et al., Case No. CGC-19-581129, Superior Court of California, San Francisco County; October 2020
- Declaration; Masood Khan v. The Greenspan Company, et al., Case No. CGC-19-581129, Superior Court of California, San Francisco County; October 2020
- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; September 2020
- Expert witness deposition; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; August 2020
- Declaration; Griffin Maclean, Inc. v. Hites and Neville, Case No. 18-2-28257-8, Washington State Superior Court, King County; August 2020
- Declaration; Griffin Maclean, Inc. v. Hites and Neville, Case No. 18-2-28257-8, Washington State Superior Court, King County; July 2020
- Declaration; Griffin Maclean, Inc. v. Hites and Neville, Case No. 18-2-28257-8, Washington State Superior Court, King County; June 2020
- Expert report; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; April 2020
- Electronic Discovery, Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 18-2-00806-29, Washington State Superior Court, Skagit County; January 2020
- Declaration; Evergreen Point Development, LLC v. Halvorson Construction Group, LLC, et al., Case No. 19-2-05329-1 SEA, Washington State Superior Court, King County; December 2019
- Declaration; Pacific Woodtech Corporation v. Daniel Semsak, Case No. 2:19-CV-01984, United States District Court for the Western District of Washington; December 2019
- Declaration; AGC Flat Glass Company North America, Inc. v. Jason Perryman, an individual, Case No. 19-CV-28663, Oregon State Circuit Court, Washington County; December 2019
- Declaration; Commercial Cold Storage, Inc. v. The City of Mt. Vernon, Washington, Case No. 19-2-00162-29, Washington State Superior Court, Skagit County; November 2019
- Declaration; Evergreen Point Development, LLC v. Halvorson Construction Group, LLC, et al., Case No. 19-2-05329-1 SEA, Washington State Superior Court, King County; November 2019
- Expert witness testimony, evidentiary hearing; Miller Construction Co., LTD v. Department of Transportation & Public Facilities, Southcoast Region, OAH No. 19-0088-CON, Alaska Office of Administrative Hearings; September 2019
- Affidavit; Law Offices of Herssein & Herssein PA v. United Services Automobile Association et al., Case No. 2015-15825-CA, Eleventh Judicial Circuit Court of Florida; August 2019
- Expert witness deposition; RJB Wholesale, Inc. v. Jeffrey Castleberry, et al., Case No. 2:16-cv-1829, United States District Court for the Western District of Washington; May 2018
- Expert report; RJB Wholesale, Inc. v. Jeffrey Castleberry, et al., Case No. 2:16-cv-1829, United States District Court for the Western District of Washington; January 2018
- Expert report; RJB Wholesale, Inc. v. Jeffrey Castleberry, et al., Case No. 2:16-cv-1829, United States District Court for the Western District of Washington; December 2017
- Affidavit; Law Offices of Herssein & Herssein PA v. United Services Automobile Association et al., Case No. 2015-15825-CA, Eleventh Judicial Circuit Court of Florida; October 2017

## Exhibit B – Leatha CV



- Affidavit; Law Offices of Herssein & Herssein PA v. United Services Automobile Association et al., Case No. 2015-15825-CA, Eleventh Judicial Circuit Court of Florida; August 2017
- Expert report; Horizon Tire Inc. (A Texas Corporation) v. Benjamin Shan, Sylvia Hermosillo, Haitao Zhang, and Flagship Tire & Wheel, LLC, Case No. 2016-03707, 127th Judicial District Court of Harris County Texas; August 2017
- Expert report; Kruger Industries, Inc. v. Sound Propeller Services, Inc., Case No. 15-2-14142-8, Washington State Superior Court, Pierce County; November 2016
- 30(b)(6) Deposition; In Re: Actos (Pioglitazone) Products Liability Litigation, MDL No. 6:11-md-2299; United States District Court for the Western District of Louisiana; March 2015
- Declaration; Shareholder Insite, Inc. v. WTAS LLC, Case No. 13-2-26202-9 SEA, Washington State Superior Court, King County; September 2013
- Declaration; In re: Oil Spill by the Oil Rig “Deepwater Horizon” in the Gulf of Mexico, on April 20, 2010; MDL 2179 Section J, United States District Court for the Eastern District of Louisiana; December 2012
- Declaration; In re: Oil Spill by the Oil Rig “Deepwater Horizon” in the Gulf of Mexico, on April 20, 2010; MDL 2179 Section J, United States District Court for the Eastern District of Louisiana; December 2011
- Expert report; In re the Marriage of Sara Stephenson and Shata Stephenson; Case No. 10-2-06746-2, Washington State Superior Court, King County; April 2011
- 30(b)(6) Deposition, In RE: Intel Corporation Microprocessor Antitrust Litigation; MDL No. 05-1717-JJF, United States District Court for the District of Delaware; March 2010
- Declaration; In RE: Intel Corporation Microprocessor Antitrust Litigation; MDL No. 05-1717-JJF, United States District Court for the District of Delaware; March 2010
- 30(b)(6) Deposition, In RE: Intel Corporation Microprocessor Antitrust Litigation; MDL No. 05-1717-JJF, United States District Court for the District of Delaware; October 2009
- Declaration; American Airlines, Inc. v. Yahoo! Inc. et al.; Case No. 4:08-CV-626-A, United States District Court for the Northern District of Texas; August 2009
- Declaration; Jerry Ryan, et al. v. Flowserve Corporation, et al.; Case No. 3:03-CV-01769-B, United States District Court for the Northern District of Texas; September 2006

## EDUCATION, CERTIFICATIONS AND LICENSES

- B.A., Environmental Studies, University of Washington, 1999
- Certificate in Computer Forensics, University of Washington, 2007
- ITIL V3 Foundation Certificate in IT Service Management, 2008
- GIAC Certified Forensic Examiner (GCFE), License 2735, 2016 – 2024
- GIAC Certified Incident Handler (GCIH), License 29294, 2017-2025

## PUBLICATIONS AND SPEAKING ENGAGEMENTS

- LegalWeek 2021; “Mitigating the eDiscovery Risks of Remote Workforces”; July 2021
- Webinar, Smarsh Inc.; “On-the-Go-Workforce: How to Stay Compliant with Mobile”; July 2020
- USSS Seattle Electronic Crimes Task Force and Washington State HTCIA; Bellevue, WA; “Cloud Forensics”; October 2019
- Webinar, Smarsh Inc.; “The Time Is Now: Understanding the Mobile Landscape”; October 2019

## Exhibit B – Leatha CV



- PREX Actionable Strategies for In-House Ediscovery; Chicago, IL; “The Changing Communication Landscape and its Impact on Ediscovery”; September 2019
- Webinar, Smarsh Inc.; “Collaboration & E-Discovery: Addressing the Challenge of Interactive Content”; May 2019
- CTIN Digital Forensics Conference at Microsoft; Redmond, WA; “Cloud Forensics”; May 2019
- Seattle University School of Law; Expert Witness Class; Mock Expert Testimony; March 2019
- CTIN General Membership Meeting; Washington State Criminal Justice Training Commission; Burien, WA; “Free and Open-Source Forensics Tools”; June 2018
- CLE; Betts Patterson Mines; Seattle, WA; “Computer forensics and eDiscovery: How to identify, preserve, review, and produce relevant sources of electronically stored information”; February 2018
- University of Washington’s OASIS: OWASP Academic Summit for Information Security; Bothell, WA; “Forensics”; May 2017
- CTIN Digital Forensics Conference at Microsoft; Redmond, WA; “Investigating Data Exfiltration”; March 2017
- CLE; King County Bar Association, Young Lawyers Division; Seattle, WA; “Investigating the Theft of Trade Secrets: The role of computer forensics in investigating the theft of trade secrets and other business confidential information”; January 2017
- Interview; The Metropolitan Corporate Counsel, “BYOD Brings Both Risks & Rewards: Considering the information governance implications of BYOD”; January 2017
- Article; The Metropolitan Corporate Counsel, “10 Key Legal Considerations for Cloud Solutions: There will be investigations and e-discovery request, are you ready?”, November 2016
- CLE Webinar; The Knowledge Group; “Social Media eDiscovery in Civil Litigation: What You Need to Know”, November 2016
- CLE Webinar; Clear Law Institute; “Behind the Curtain: What else is hidden in your social media?”, November 2016
- CLE Webinar; Cost Effective eDiscovery Solutions at Lewis Brisbois; “E-Discovery Trends, Rules and Tips”; May 2016
- CTIN 2016 Digital Forensics Conference; Washington State Criminal Justice Training Commission; Burien, WA; “Windows Event Log Forensics”; March 2016
- CLE; King County Bar Association, Young Lawyers Division; Seattle, WA; “Digital Evidence: How Electronically Stored Information May Impact Your Next Case”; January 2016
- CLE Webinar, The Knowledge Group; “Emerging Issues: Reconsidering Intellectual Property in Cloud Computing in 2016”; November 2015
- CLE Webinar, Cost Effective eDiscovery Solutions at Lewis Brisbois; San Francisco, CA; “Effective preservation, analysis and review of data stored on mobile devices”, October 2015
- CTIN Digital Forensics Conference; Washington State Criminal Justice Training Commission; Burien, WA; “IP Theft Investigations; A detailed look at the tools and techniques used for intellectual property theft investigations”, March 2015
- CLE; King County Bar Association, Young Lawyers Division; Seattle, WA; “General Discussion on Social Media and Its Impact on e-Discovery”; December 2014
- CLE; Bracewell & Giuliani LLP; Seattle, WA; “General Discussion on Social Media and Its Impact on e-Discovery”; October 2014
- CTIN Digital Forensics Conference; Washington State Criminal Justice Training Commission; Burien, WA; “Mobile Device Forensics: Application Analysis Tools and Techniques”, March 2014

## Exhibit B – Leatha CV



- The Masters Conference; San Francisco, CA; “Cloud Computing and Mobile Devices: How to be Prepared for Litigation”, March 2014
- CLE; Bingham McCutchen; San Francisco, CA; “Cloud Computing and Mobile Devices: How to be Prepared for Litigation”, March 2014
- Article; The Metropolitan Corporate Counsel, “Mobile Device Forensics: The New Frontier”, January 2014
- Computer Technology Investigators Network, Webinar; “Analysis of Email Metadata”, June 2011
- Washington State Association for Justice (WSAJ) CLE; Seattle, WA; “Looking in the Right Places: Uncovering where companies keep electronic information”, October 2009
- Texas State Bar CLE, Electronic Discovery and Digital Evidence Institute; Houston, TX; “Focus on E-Mail Evidence” and “Panel Discussion: Q & A on Search”, April 2009
- West LegalWorks CLE; Chicago, IL; “E-Discovery Searching Techniques and Tools”, October 2005

## PROFESSIONAL AFFILIATIONS

- Sedona Conference Working Group on Electronic Document Retention and Production (WG1); 2005 – present
- Sedona Conference Working Group on Data Security and Privacy Liability (WG 11); 2014 - present
- Computer Technology Investigators Network (CTIN); 2009 – present
- Board Member, Computer Technology Investigators Network (CTIN); 2014 – present
- SANS GIAC Advisory Board; 2016 – present
- Information Systems Security Association (ISSA), Puget Sound Chapter; 2016 – present
- Board Vice President, Information Systems Security Association (ISSA), Puget Sound Chapter; 2020 – present

**Exhibit C – Former Mayor Durkan’s Deleted Text Messages**

Deleted Message Count	Previous Message Date (PT)	Following Message Date (PT)	Deletion Type
5746	Unknown	6/25/20 10:38:48 AM	30-day Retention Setting
11	6/25/20 12:33:43 PM	6/26/20 6:43:14 AM	Manual User Deletion
1	6/26/20 9:08:57 AM	6/26/20 10:41:09 AM	Manual User Deletion
4	6/30/20 8:38:02 AM	6/30/20 12:07:09 PM	Manual User Deletion
7	6/30/20 12:07:52 PM	6/30/20 9:27:21 PM	Manual User Deletion
3	7/1/20 11:45:10 AM	7/2/20 12:16:00 AM	Manual User Deletion
1	7/2/20 9:49:06 AM	7/2/20 9:58:34 AM	Manual User Deletion
2	7/2/20 9:58:34 AM	7/2/20 6:28:56 PM	Manual User Deletion
1	7/5/20 11:59:58 AM	7/6/20 2:10:07 PM	Manual User Deletion
3	7/6/20 10:45:12 PM	7/7/20 8:22:59 AM	Manual User Deletion
1	7/7/20 8:24:15 AM	7/7/20 8:28:15 AM	Manual User Deletion
1	7/7/20 8:28:15 AM	7/7/20 8:28:51 AM	Manual User Deletion
3	7/7/20 8:28:51 AM	7/7/20 8:37:38 AM	Manual User Deletion
4	7/7/20 8:43:46 AM	7/7/20 1:19:31 PM	Manual User Deletion
1	7/7/20 1:38:56 PM	7/7/20 5:04:18 PM	Manual User Deletion
4	7/7/20 5:05:31 PM	7/7/20 8:33:04 PM	Manual User Deletion
4	7/8/20 6:48:13 AM	7/8/20 8:36:35 PM	Manual User Deletion
5	7/10/20 8:54:35 AM	7/10/20 10:00:54 AM	Manual User Deletion
4	7/10/20 11:28:49 AM	7/11/20 6:50:45 AM	Manual User Deletion
1	7/11/20 7:28:12 PM	7/12/20 12:00:55 PM	Manual User Deletion
1	7/12/20 1:03:08 PM	7/12/20 1:04:14 PM	Manual User Deletion
1	7/17/20 5:52:41 AM	7/17/20 11:43:38 AM	Manual User Deletion
10	7/19/20 5:02:45 PM	7/20/20 8:56:19 AM	Manual User Deletion
4	7/20/20 10:43:35 AM	7/20/20 11:04:28 AM	Manual User Deletion
1	7/21/20 1:45:36 PM	7/21/20 3:48:13 PM	Manual User Deletion
1	7/21/20 3:59:27 PM	7/21/20 11:54:23 PM	Manual User Deletion
5	7/22/20 5:01:30 AM	7/22/20 8:05:03 AM	Manual User Deletion
1	7/22/20 8:05:03 AM	7/22/20 8:45:45 AM	Manual User Deletion
6	7/22/20 8:45:45 AM	7/22/20 10:16:24 AM	Manual User Deletion
6	7/22/20 10:17:15 AM	7/22/20 12:54:05 PM	Manual User Deletion
1	7/22/20 12:55:07 PM	7/22/20 1:13:47 PM	Manual User Deletion
13	7/22/20 2:15:28 PM	7/22/20 6:03:04 PM	Manual User Deletion
1	7/23/20 5:41:10 PM	7/23/20 7:02:28 PM	Manual User Deletion
1	7/27/20 8:27:19 PM	7/27/20 8:29:53 PM	Manual User Deletion
4	7/28/20 1:13:51 PM	7/28/20 4:06:23 PM	Manual User Deletion
1	7/29/20 10:24:09 AM	7/29/20 11:36:03 AM	Manual User Deletion
2	8/1/20 8:36:45 PM	8/1/20 11:07:58 PM	Manual User Deletion
4	8/2/20 9:19:32 PM	8/2/20 10:24:38 PM	Manual User Deletion
2	8/2/20 10:24:38 PM	8/3/20 8:35:06 AM	Manual User Deletion
11	8/3/20 10:38:24 AM	8/4/20 8:21:03 AM	Manual User Deletion

**Exhibit C – Former Mayor Durkan’s Deleted Text Messages**

<b>Deleted Message Count</b>	<b>Previous Message Date (PT)</b>	<b>Following Message Date (PT)</b>	<b>Deletion Type</b>
2	8/5/20 4:34:21 PM	8/5/20 6:08:55 PM	Manual User Deletion
2	8/13/20 9:05:30 PM	8/14/20 10:40:24 AM	Manual User Deletion
1	8/19/20 6:44:57 AM	8/19/20 9:50:07 AM	Manual User Deletion
1	8/25/20 10:10:21 AM	8/25/20 8:03:17 PM	Manual User Deletion
1	8/25/20 8:03:17 PM	8/26/20 9:55:13 PM	Manual User Deletion
9	8/26/20 9:57:56 PM	8/29/20 2:20:36 PM	Manual User Deletion
5	8/29/20 9:39:59 PM	8/29/20 10:37:08 PM	Manual User Deletion
1	8/31/20 4:57:40 PM	9/1/20 7:57:45 AM	Manual User Deletion
1	9/1/20 4:32:11 PM	9/1/20 4:43:43 PM	Manual User Deletion
3	9/1/20 5:23:38 PM	9/1/20 5:56:05 PM	Manual User Deletion
1	9/2/20 8:59:14 PM	9/2/20 9:32:17 PM	Manual User Deletion
3	9/3/20 9:43:56 AM	9/3/20 2:10:38 PM	Manual User Deletion
2	9/4/20 7:04:03 AM	9/5/20 8:31:42 AM	Manual User Deletion
1	9/5/20 8:35:11 AM	9/6/20 3:13:42 PM	Manual User Deletion
8	9/8/20 9:40:21 PM	9/9/20 2:12:42 PM	Manual User Deletion
1	9/9/20 2:12:42 PM	9/9/20 2:13:27 PM	Manual User Deletion
1	9/9/20 2:15:32 PM	9/9/20 2:16:14 PM	Manual User Deletion
8	9/9/20 2:19:06 PM	9/9/20 6:51:53 PM	Manual User Deletion
1	9/22/20 8:59:46 AM	9/22/20 9:03:24 AM	Manual User Deletion
1	10/21/20 8:05:47 AM	10/21/20 8:15:28 AM	Manual User Deletion
1	11/16/20 12:32:23 PM	11/16/20 2:27:39 PM	Manual User Deletion