Cellebrite Digital intelligence for a safer world

Date: April 8th, 2021

TO WHOM IT MAY CONCERN,

This letter is to confirm that Cellebrite DI Ltd., acting through its United States-based subsidiary, Cellebrite Inc., is the sole manufacturer of all Cellebrite products. Cellebrite Inc. is the only provider of Cellebrite services, including product support and Cellebrite Advanced Services (CAS), in North America.

Cellebrite Inc., established in 1999 and based in Parsippany, NJ, is incorporated in the state of Delaware. Cellebrite Inc. supports customers and users in the US and Canada.

CAS is a unique offering that is available only from Cellebrite on-site, or via drop off at or shipment to one of our Cellebrite Forensics Labs (CBFL) in Vienna, VA, Parsippany, NJ, or Ottawa, ON.

Listed below are the service offerings:

Service Options:

- Per device basis – onetime fee for Advanced Unlocking and/or Advanced Extraction, plus shipping and handling charges
- Subscription – annual fee for unlimited phone submissions for Advanced Unlocking and/or Advanced Extraction, including shipping and handling charges, with a maximum number of concurrent phones allowed to be in process at the CBFL

Apple iOS Unlocking & Extraction Capabilities:

Apple iPhone 4S/5/5c/5S/6/6+/6S/6S+/SE/7/7+/8/X/XR/XS/11

- Only service solution in the world for all versions of iOS 5.x to iOS 14.x
- Only service solution in the world to provide full file system extraction
- Unlocking and extraction from iPhone, iPad, & iPod Touch devices
- No jailbreak required, fully forensic process for unlocking and extraction
- Un-disable (Disabled, Connect to iTunes) possible for most devices

Samsung Android Unlocking and Extraction Capabilities:

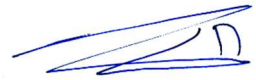
Samsung Decrypted Extraction (Bypass/Disable/Determine Screen Lock or Determine Secure Startup Passcode or Determine File-Based Encryption Passcode) for Galaxy S6, S7, S8, S9, S10, S20, Note 5, Note 8, Note 9, Note 10, Note 20 (plus many mid-range and low-end models)
Only service solution in the world to:

- Bypass bootloader lock, factory reset protection (FRP), and reactivation lock
- Extract a decrypted physical image (Full Disk Encryption) or full file system (File-Based Encryption) of the device memory
- Extract the encrypted contents of Secure Folder

Other Android Unlocking and Extraction Capabilities:
Support for many other locked and/or encrypted Alcatel, Asus, Google, HTC, Huawei, Kyocera, LG, Motorola, Nokia, OnePlus, OPPO, Sony, Vivo, and Xiaomi devices running Android versions 4.4 to 11, on a case-by-case basis when they are not supported by Cellebrite Universal Forensic Extraction Device (UFED), including Qualcomm Emergency Download (EDL) supported devices with Secure Startup enabled.

Please feel free to contact Cellebrite with any questions.

Sincerely,



Hagit Reuven
VP, Sales Operations

May 2021

TO WHOM IT MAY CONCERN,

This letter is provided to inform you that a **Sole Source justification** exists because the solution identified in this document, required to satisfy the Agency's needs, are only manufactured, developed or made available from Cellebrite Inc. This letter identifies Cellebrite Inc. As the sole Developer, and Manufacturer of respective items listed below in detail:

Cellebrite Premium

Cellebrite Inc. was established in 1999 and is based in Parsippany, NJ and Vienna, VA, and is incorporated in the state of Delaware. Cellebrite Inc. supports customers and users in the US, Latin America, Canada and Mexico. With more than 60,000 extraction licenses deployed in 150 countries, Cellebrite' s forensic extraction products have been deployed throughout the world, and our Cellebrite Analytics Enterprise Product is an extension of these forensic extraction products. Our forensic extraction customers include the Department of Defense, Federal Government, Intelligence Organizations, Military, and Law Enforcement Divisions.

Cellebrite Premium has capabilities that are exclusive to Cellebrite and not available from any other company. No other solution can unlock and extract both Android and iOS devices. As Mobile devices play a major role during investigations, Cellebrite Premium technology provides Law Enforcement personnel access to the newest locked, encrypted, and updated Mobile devices. This capability enables the Law Enforcement to collect digital evidence such as phone logs, chat messages, emails, images and other information that is locked and encrypted.

Our competitive advantages include:

• **Access Locked and Encrypted leading mobile devices.** Cellebrite Premium supports Full File-System and Physical extraction from the widest range of iOS and Android devices while bypassing, After-First-Unlocking or brute forcing the device passcode and other security measures. Cellebrite Premium is the

only tool that provides both a Generic iOS and Generic Android devices in the same product. Premium support all the leading vendors in the market including Apple, Samsung, Huawei, Motorola, LG, OPPO, VIVO, Google, Sony, Xiaomi and many others.

In addition, Cellebrite Premium provide access (extraction and decoding) to leading Android secured containers such as Samsung secured folder, Huawei Private Space and Xiaomi 2nd Space.

• **Large, Established User Community.** Since 2007, Cellebrite has deployed more than 60,000 Cellebrite UFED in 100+ countries to support law enforcement, intelligence services, border patrols, military forces, public safety agencies and commercial organizations.

• **Industry's Broadest Device & App Support.** Cellebrite has the largest device inventory in the industry that holds more than 15K mobile devices from different vendors, OS, Locations and years. Cellebrite is purchasing dozens of devices each month from different countries to support customer's needs.

• **Forensically Sound Evidence Every Time.** Unlike competitors' "black box" third-party boot loaders or other tools, Cellebrite Premium uses custom-designed, read-only methods, which ensure forensically sound File-System and Physical extractions.

• **Technology and Research and Development (R&D) Leadership.** Cellebrite provides the mobile forensic industry's most comprehensive Android, Apple iOS, Blackberry, and Windows Mobile support. Cellebrite has a staff of 250+ engineers—the most of any mobile forensics' solution provider. We are committed to investing in the ongoing R&D to innovate around customer and market needs.

• **Best-in Class Training Ensures a Repeatable, Reproducible Mobile Forensics Process.** Open to all user levels, from beginners to advanced, Cellebrite certification training provides hands-on experience with Cellebrite products and applications, delivering the tools and knowledge required for evidence collection data analysis, searching, and reporting.

Sincerely,

Hagit Reuven

VP, Sales Operations

Cellebrite Digital intelligence for a safer world

Date: March 16th, 2020

TO WHOM IT MAY CONCERN,

This letter is to confirm that Cellebrite DI Ltd., acting through its United States-based subsidiary, Cellebrite Inc., is the **sole manufacturer** and developer of the Universal Forensic Extraction Device (UFED) Mobile Forensics solution.

Cellebrite Inc., established in 1999 and based in Parsippany, NJ, is incorporated in the state of Delaware. Cellebrite Inc. supports customers and users in the US and Canada.

The UFED is a mobile forensics extraction, decoding, and analysis tool that extracts logical, file system, and physical data from mobile devices (i.e., smartphones, cell phones, tablets, GPS units, SIM cards, memory cards, drones and USB devices), including live and deleted data, contacts, phone numbers, call logs, text messages, SMS messages, app data (social network and other), location data, pictures, videos, and voice messages.

UFED technology provides digital forensic lab examiners, investigators, field personnel, and first responders with the capability to collect, protect and act decisively on mobile device data with the speed and accuracy a situation demands. Our competitive advantages include:

- **Large, Established User Community.** Since 2007, Cellebrite has deployed more than 40,000 UFEDs in 100+ countries to support law enforcement, intelligence services, border patrols, military forces, public safety agencies and commercial organizations.
- **Industry's Broadest Device & App Support.** Cellebrite has established collaborative business relationships with original equipment manufacturers (OEMs) and wireless carriers worldwide. These global partners send us more than 100 new handsets per month - most prior to actual consumer market release. This allows Cellebrite Mobile Forensics to develop mobile forensics support for new devices prior to our competition. We retain more than 8,000 mobile phones at our company headquarters for ongoing innovation and support.
- **Technology and Research and Development (R&D) Leadership.** Cellebrite provides the mobile forensic industry's most comprehensive Android, Apple iOS, Blackberry, and Windows Mobile support. Cellebrite has a staff of 250+ engineers—the most of any mobile forensics solution provider. We are committed to investing in the ongoing R&D to innovate around customer and market needs.
- **Best-in Class Training Ensures a Repeatable, Reproducible Mobile Forensics Process.** Open to all user levels, from beginners to advanced, Cellebrite certification training provides hands-on experience with Cellebrite products and applications, delivering the tools and knowledge required for evidence collection data analysis, searching, and reporting.
- **Physical and Full File System Extraction with Lock Bypass.** Cellebrite supports physical extraction while from more than 8,034 different device types, including Android (1000+ devices from Samsung, Huawei, LG, Motorola, and other vendors); Apple iOS; and Windows Phone (Nokia and Lumia). Cellebrite supports more than 8000 devices for full file system extraction including File-based- encryption devices up to the latest Samsung Flagships (S20, S21) and devices running Android 11 .
- **Forensically Sound Evidence Every Time.** Unlike competitors' "black box" third-party boot loaders, UFED uses custom-designed, read-only boot loaders, which ensure forensically sound file system and physical extractions

UFED technology includes capabilities that are exclusive to Cellebrite and not available from any other company.

Exclusive Android Capabilities

- Qualcomm live - The new capability extends access to the latest devices from vendors such as Xiaomi, OPPO, OnePlus, VIVO, Nokia, LG Motorola and others, running OS versions 7 up to 11. This is a generic full file system extraction for unlocked Qualcomm based Android devices across many vendors and up to the latest Android version, Android 11. including devices such as: S10, Note 10, Note 9, S9, Note 8, S8 , S20 and others.
- Support full file system extraction for Samsung Exynos devices including latest Flagships such as Samsung S20 and S21 running Android 11 (Industry first).
- Support for selective file system extraction to directly collect specific applications or files, which will save valuable time during investigations and will allow investigators to collect just what they need or allowed to, with minimal privacy intrusion.
- Support for an automated screen capturing process for Android devices. The fully automatic flow allows users to select specific chat conversation while defining specific time frames. The fully automated flow includes support for WhatsApp, Signal, Instagram and SnapChat applications.
- Decrypted physical extraction of data from Samsung Galaxy S6, Galaxy Note 5 and some Galaxy S7 devices
  Decrypting EDL - Lock-bypassing decrypted physical extraction capability for Qualcomm Android devices. Widely supported chipsets: 8909, 8916, 8939, 8952, 8936, 8917, 8937, 8940 & 8953), including Huawei H1611, Xiaomi Mi 5, ZTE Z832 Sonata 3, ZTE Z956 Grand X 4, Xiaomi Redmi 4 Hot, Motorola XT1765 Moto E MetroPCS and ZTE Z981 ZMax Pro, including devices running the latest Qualcomm chipsets ().
- Physical extraction and unlocking capabilities for Samsung devices! Extended support to more than 100 Exynos and Qualcomm devices including: Galaxy S7 Edge, S7, S6 Edge, S6 Edge+, Note 5, A5 and J7 families.
- Automatically bypass locked Android devices with LockPick – lock bypass capability across a broader range of Android devices including Samsung flagship devices.
- An Industry First – Samsung Exynos Physical Bypass Solution – This unique capability enables unlock, full file system and physical extractions from popular Samsung devices with the Exynos processor. Supported devices include: SM-G930F Galaxy S7, SM-G935F Galaxy S7 Edge, SM-A520F Galaxy A5 2017 and SM-J730F Galaxy J7 Pro.
- Exclusive access to evidence from locked and encrypted low to mid-end Samsung devices with Qualcomm chipsets. The devices include: J3 (J327P, J327VL), J7 (J727V, J727P) & A9 (A9100, A9000). Chipsets include: 8917, 8937, 8953 & 8976.
- An industry-first new solution for removing screen lock on 64 LG Android Devices. Users can now disable and remove the screen lock to gain access to critical evidence from some of the most popular and advanced LG Android-OS devices including H870 G6, H820 G5, LM-X210MA, M210, MP260 and more.
- First-to-market access to 87 locked and encrypted Android devices running the latest MediaTek chipsets (6757,6755,6797,6735,6750,6737,6753,6580).
- Partial file system extraction while bypassing screen lock for 105 Android Samsung devices, including devices running on Android 6 OS
- Bootloader-based physical bypass extraction support for 48 of the toughest locked Qualcomm-based Android devices, and 33 Android devices using ADB method. This unique unlocking method supports devices based on the MSM8909, MSM8916, MSM8936, MSM8939, and MSM8952 chipsets from EDL (Emergency Download) mode. Supported Android devices include: HTC Desire: 510/620/826, Alcatel One Touch Pixi, Vivo X5/X7, Motorola XT1526 and XT1543.
- Exclusive Huawei Decrypting Bootloader Capability – New generic capability enables Lock-bypassing Physical and Full File System extractions for dozens of Huawei devices (including P10, Mate 10 and P9), equipped with HiSilicon Kirin chipsets from the following families: 92x, 93x, 95x, 96x.
- Lock Screen Removal (Disable User Lock) for 71 high/mid-tier Samsung Android devices. Supported devices include SM-G935T Galaxy S7 Edge, SM-J710FN Galaxy J7, SM-A700YD Galaxy A7 Duos and SM-A500W Galaxy A5
- New disable user lock capabilities have been added to 65 supported LG devices, including prepaid devices: L52VL Treasure, L15G Sunrise, LGL22C Power and LGL41C Ultimate 2

- Physical and file system ADB extractions for 51 Samsung Android devices, including SM-G935FD Galaxy S7 Edge, SM-G920T Galaxy S6 and SM-G930F Galaxy S7
- Built-in Android temporary root (granting extra permissions) for hundreds of Android devices
- Physical extraction while bypassing user lock on 140 LG devices, including the G3 and G4
- Bypass user screen lock for 137 Samsung devices, including the Galaxy S5, Tab and Galaxy Note 2, 3, and 4

Exclusive Apple (iOS) capabilities

- Full File system extraction from iPhone 5 – iPhone X. With a Built-in Solution Based on checkm8, examiners can take advantage of a first-to market solution. This solution allows users to quickly perform a forensically sound temporary jailbreak and full file system extraction within one streamlined workflow.
- Ability to take a screenshot automatically from the iOS device
- Decrypted physical extraction of data from Apple iPhones 4S, 5, 5c
- Full file system extraction of data from Apple devices (5/5c/6/6 plus)
- iOS unlocking support for Apple devices (4s/5/5c/6/6 plus) running iOS 8.x - 10.x, with no risk of a device wipe
- iOS unlocking support for Apple devices (5/5c/6/6 plus/7/7 plus/8/8 plus/x) running iOS 11.x, with no risk of a device wipe
- UFED User Lock Recovery Tool (iOS)

Exclusive Blackberry Capabilities

- BlackBerry 10 file system extraction, backup acquisition & decryption
- Physical extraction for unlocked BlackBerry 7xxx/8xxx/9xxx devices (including NAND and NOR memory)

Other Exclusive Capabilities

- Cellebrite offers the ability to manage all units and licenses using Cellebrite central management system, Cellebrite Commander. The solution can integrate with the central management platform that can oversee usage, permissions, SOPs, configurations, licensing, and SW updates.
- Document user actions and Incorporate Investigative Notes - As part of the digital data extraction and collection process, users can add notes, include observations or report any issues encountered during the process. This capability is an effective way to maintain an audit trail documenting actions and decisions taken along the way. In addition to user notes UFED can also include a customizable agency form (e.g. Consent form) to be used as part of the data collection process.
- Insights from installed apps - The solutions offer the ability to present, prior to the extraction process, a list of installed applications divided to categories with an overview for each application and highlight ones that could be relevant for criminal investigation.
- Dynamic profiles: The dynamic profiles mechanism enable to create on-the-fly profiles for phone models which were not formally approved in our lab. To keep you on track with the latest capabilities, the UFED solution suggests additional available methods based on our unique capabilities database. Users will see the new methods labelled Untested.
- Physical extraction with password bypass for Nokia Lumia Windows Phone 8 devices, including the Lumia 520, 820, 822, 920, 928, and 1020
- Physical extraction while bypassing user lock for 3 Nokia 105 devices: RM-1133, RM-1134 and RM-1135
- Physical extraction while bypassing user lock and decoding support for 37 Huawei devices (Hisilicon)
- Physical extraction and decoding support for the latest TomTom devices, including the Go 1000 Point Trading and 4CQ01 Go 2505 Mm
- Provide support matrix – what is supported using username and password / application token.
- Provide traces and changes document that describe what traces the extraction process might leave.
- Supports extracting a token from the subject device in addition to the user name and password option for several of data sources including; Facebook, WhatsApp, Twitter, Gmail, Google(Location History, My Activity, Photos,

Chrome, Calendar, Contacts, Drive, Bookmarks, Tasks), Mail (IMAP), Dropbox, iCloud(App, Calendar, Contacts, Drive, Photos, OneDrive, Notes, Reminder, Location), Instagram, VK, Telegram and more

Please feel free to contact Cellebrite with any questions.

Sincerely,

Hagit Reuven
VP, Sales Operations