UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FINCO SERVICES, INC., Plaintiff, v. FACEBOOK, INC., CALIBRA, INC., JLV, LLC and CHARACTER SF, LLC, Defendants.	CASE NO. 1:19-cv-09410 (PKC) (KHP) **JOINT STIPULATION AND [PROPOSED] ORDER RE: DISCOVERY OF ELECTRONICALLY STORED INFORMATION**

1. PURPOSE

This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure, and any other applicable orders and rules. The parties and the Court recognize that this Joint Stipulation and [Proposed] Order is based on facts and circumstances as they are currently known to each party, that the electronic discovery process is iterative, and that additions and modifications to this Joint Stipulation and [Proposed] Order may become necessary as more information becomes known to the parties.

For the avoidance of doubt, this stipulation is limited to e-discovery; nothing herein shall relieve the parties of the duty to conduct a reasonable search for hard copy documents in response to a requesting party's discovery requests in accordance with the Federal Rules of Civil Procedure. And nothing in this ESI stipulation shall waive in whole or in part any objection raised by a party in connection with specific discovery requests served in this action.

2. COOPERATION AND PROPORTIONALITY

The parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith throughout the matter consistent with this Court's Guidelines for the Discovery of ESI to promote the "just, speedy, and inexpensive determination" of this action, as required by Fed. R. Civ. P. 1. The parties are expected to use reasonable, good faith and proportional efforts to preserve, identify and produce relevant and discoverable information consistent with Fed. R. Civ. P. 26(b)(1). This includes identifying appropriate limits to discovery, including limits on custodians, identification of relevant and discoverable subject matter, time periods for discovery, and other parameters to limit and guide preservation and discovery issues. The failure of counsel or the parties to cooperate in facilitating and reasonably limiting discovery requests and responses will be considered in cost-shifting determinations.

3. LIAISON

Each party shall designate an individual or individuals as e-discovery liaison(s) who must:

(a) be prepared to meet and confer on discovery-related matters and to participate in discovery dispute resolution;

(b) be knowledgeable about the party's discovery efforts; and

(c) be, or have reasonable access to those who are, familiar with the party's electronic systems and capabilities in order to explain those systems and answer relevant questions; and be, or have reasonable access to those who are, knowledgeable about the technical aspects of e-discovery, including electronic document storage, organization, and format issues, and relevant information retrieval technology, including search methodology.

4. PRESERVATION

Each party is responsible for taking reasonable and proportionate steps to preserve relevant and discoverable ESI within its possession, custody or control consistent with Sedona Conference Principle 6 which instructs that "[r]esponding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically

stored information."[1] The parties have discussed their preservation obligations and needs and agree that preservation of potentially relevant ESI will be reasonable and proportionate. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

(a) Parties shall preserve non-duplicative, discoverable information in their possession, custody or control. Parties, however, shall not be required to modify the procedures used by them in the usual course of business to back-up and archive data, such as automatic email back-up or other archival systems.

(b) Subject to and without waiving any protection described in Section 4(a) above, the parties agree that:

1. Only ESI created or received after June 1, 2018 will be preserved;
2. The parties shall agree on the custodians for whom they believe ESI should be preserved, including the addition of additional custodians as necessary;

(c) These data sources are not reasonably accessible because of undue burden or cost pursuant to Fed. R. Civ. P. 26(b)(2)(B) and ESI from these sources will be preserved pursuant to normal business retention, but not searched, reviewed, or produced, unless otherwise ordered by the Court upon a motion of a party:

1. backup systems and/or tapes used for disaster recovery; and
2. systems no longer in use that cannot be accessed.

(d) Among the sources of data the parties agree are not reasonably accessible, based on mutual representation of the parties' counsel, the parties agree not to preserve, collect, process, review and/or produce the following:

1. Deleted, slack, fragmented, or unallocated data only accessible by forensics.
2. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

[1] The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 SEDONA CONF. J. 118 (2018).

3. On-line data such as temporary internet files, history, cache, cookies, and the like.
4. Data in metadata fields that are frequently updated automatically, such as last-opened dates.
5. Back-up data that are substantially duplicative of data that are more accessible elsewhere.
6. Voice messages.
7. Instant messages and chats that are not chronicled to an email archive system.
8. Sound recordings, including, without limitation, .mp3 and .wav files
9. Video recordings
10. Electronic data (e.g. email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), provided that a copy of all such electronic data is routinely saved elsewhere (such as on a server, laptop, desktop computer, or "cloud" storage).
11. Mobile device activity logs
12. Server, system, or network logs.
13. Dynamic fields in databases or log files not stored or retained in the usual course of business.
14. Data remaining from systems no longer in use that is unintelligible on the systems in use.
15. Information created or copied incidental to the deployment, maintenance, retirement, and/or disposition of computer equipment by the party, such as incidental copies of a hard drive made when information is transferred from an old, retired device to a new device.

16. Other forms of ESI whose preservation requires unreasonable, disproportionate, and/or non-routine, affirmative measures that are not utilized in the ordinary course of business.

5. SEARCH

(a) The parties agree that in responding to an initial Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery.

(b) Nothing in this Order shall be construed or interpreted as precluding a producing party from performing a responsiveness review to determine if documents captured by search terms are in fact relevant to the requesting party's request. Further, nothing in this Order shall be construed or interpreted as requiring the production of all documents captured by any search term if that document is in good faith and reasonably deemed not relevant to the requesting party's request.

(c) Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list.

(d) De-Duplication. Each party is required to produce only a single copy of a responsive document and each party may de-duplicate responsive ESI (based on MD5 hash values at the document level) across Custodians. For emails with attachments, the hash value is generated based on the parent/child document grouping. To the extent that de-duplication through MD5 hash values is not possible, the parties shall meet and confer to discuss any other proposed method of de-duplication.

(e) Email Threading. Where multiple email messages are part of a single chain or "thread," a party is only required to produce the most inclusive message ("Last In

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.