UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

PAUL D. CEGLIA, Plaintiff, v. MARK ELLIOT ZUCKERBERG and FACEBOOK, INC., Defendants.	Civil Action No. 1:10-cv-00569-RJA **DECLARATION OF MICHAEL F. MCGOWAN IN SUPPORT OF DEFENDANTS' MOTION FOR EXPEDITED DISCOVERY**

I, Michael F. McGowan, declare and state as follows:

Introduction

1. Stroz Friedberg, LLC ("Stroz Friedberg") has been retained by Gibson, Dunn & Crutcher, LLP ("Gibson Dunn"), on behalf of its clients Mark Zuckerberg and Facebook, Inc. ("Facebook"), in the above-styled case to provide consulting and electronic discovery services and to conduct digital forensic examinations of various media. This declaration is executed by Michael F. McGowan, a Director of Digital Forensics at Stroz Friedberg. I have helped lead the development of Stroz Friedberg's expertise in detecting backdating and forgeries of electronic documents.

2. I have been informed by Gibson Dunn that Paul Ceglia claims to possess a contract between himself and Mr. Zuckerberg regarding "The Face Book" that Mr. Ceglia prepared and saved on his computer (the "Purported Contract"), as well as email messages between Mr. Ceglia and Mr. Zuckerberg regarding the ownership of "The Face Book" (the "Purported Emails"). I also have been informed that Mr. Zuckerberg and Facebook maintain that these documents are fabricated in whole or in part. I further have been informed that Mr. Ceglia claims to have recently discovered the existence of the Purported Emails on computers in his parents' home.

3. As set forth below, Stroz Friedberg has extensive experience and is a leading expert in assessments as to whether electronic documents have been backdated, forged, or altered. As explained below, to best make such assessments, Stroz Friedberg needs to inspect: (a) all native electronic versions of the Purported Contract and the Purported Emails; and (b) every available computer or piece of external media on which the electronic documents in question were created, viewed, saved, or modified. As explained below, there can be substantial information in the native electronic versions of the files in question that bear on their authenticity. Producing printouts, Adobe Acrobat .pdf files, or other similar non-native copies of the documents do not give a digital forensic examiner comparable access to the critical existing evidence bearing on authenticity.

4. In addition, as explained below, evidence relating to authenticity can be extracted from many locations on any computers on which the documents in question were created, saved, viewed, or modified. These locations include the computer system, application, and security logs; the unallocated space of the computers from which deleted files or file fragments may be recovered; the portion of the hard drives that stores the dates and times that files were created, last accessed, and modified; and the files that show what documents recently were accessed.

5. Accordingly, this declaration is in support of Gibson Dunn's motion for expedited discovery requiring Mr. Ceglia to produce for forensic preservation and unfettered digital forensic analysis: (a) all native electronic versions of the Purported Contract and the Purported Emails; and (b) all computers and electronic media within Mr. Ceglia's possession, custody, or control, including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies. As further described below, creating forensically-sound copies of this native data and these computers and electronic media is critical to performing an assessment of whether the Purported Contract and the Purported Emails are legitimate or the product of fraud.

Qualifications in E-Forgery Matters

6. I have gained expertise through experience, research, and training in detecting e-forgeries. I have conducted digital forensic examinations of multiple computers, external hard drives, and other digital media in both routine cases and cases in which many millions of dollars or people's freedom have hinged on the authenticity of proffered electronic documents. In many cases, I have been able to find critical evidence that bore on the authenticity of the electronic documents and, in a majority of the cases, that evidence has resolved the matter.

7. I am a Director of Digital Forensics at Stroz Friedberg. I co-manage Stroz Friedberg's technical operations in the areas of digital forensics and cyber-crime response. I have conducted hundreds of digital forensic examinations and data acquisitions from various media types, including laptop and desktop computers, servers, and mobile devices. I also have been the lead digital forensic examiner on most of the firm's significant e-forgery investigations. I have provided trial and hearing testimony on a number of occasions and have been admitted as an expert in digital forensics in federal and state court, including on behalf of the United States Department of Justice in connection with one of the Enron Task Force prosecutions. A copy of my C.V. is attached to this declaration as Exhibit A.

8. On this matter, I worked under the direction and supervision of Eric M. Friedberg. Mr. Friedberg is Co-President of Stroz Friedberg. He has participated in and supervised hundreds of digital forensics examinations over his past eleven years with Stroz Friedberg, both in the context of litigation-related disputes and responses to cyber-crime. He has participated in and supervised almost all of the firm's e-forgery matters, including those on which I was the lead digital forensics examiner. These e-forgery matters have involved disputes over the authenticity of contracts, e-mails, movie scripts, and memoranda. He has published an article and lectured on

e-forgery. Prior to joining Stroz Friedberg, Mr. Friedberg was an Assistant United States Attorney with the United States Attorney's Office for the Eastern District of New York from 1989 to 2000. Mr. Friedberg acted at various times as the Office's Chief of Narcotics and the district's lead cyber-crime prosecutor. A copy of Mr. Friedberg's C.V. is attached to this declaration as Exhibit B.

Conducting the Authenticity Analysis

A. Information Available from the Native Electronic Files

9. In an authenticity case, it is critically important for a digital forensic expert to have available for examination more than the paper printouts or images (.pdf or .tiff files) of the documents. A digital forensic examiner should have full access to every available version of the "native" electronic files at issue, meaning the format in which the file was originally created. For example, email stored by a user using Microsoft Outlook should be produced in Outlook format, normally in a file called a ".pst file". As another example, Microsoft Word documents should be produced as Word documents (.doc or .docx files). If a Word document has been rendered as a .pdf file, then the Word version and the .pdf version should be produced.

10. Native electronic documents contain certain data about the creation and use of the documents. This data is called "embedded metadata" and can include information about the date the document was created, last accessed, modified, and printed; the author of the document; the name of the user who last opened the document; the date an email was sent or modified; and other information. This data can be critical in authenticating a document, as anomalies in this metadata can constitute clear proof of backdating or fraudulent editing.

11. Native emails also contain many embedded metadata attributes that are useful in determining authenticity. Some of that embedded metadata is immediately visible on the face of

an email, such as the sender of the email, the recipients of the email, the date and time the email was sent or received, and the subject of the email. However, a digital forensic examination of an email produced in native format can reveal other useful embedded metadata, such as the Internet headers. When an email is transmitted across the Internet from the sender to the recipient, each server that is used in the transmission affixes the date and time at which the email was received by the server to the email's Internet headers metadata. Anomalies in the Internet headers can readily reveal backdating and fraud. An analysis of email Internet headers, including the date and time stamping, is critical in a case such as this where Mr. Ceglia is claiming that key emails were exchanged over the Internet between him and Mr. Zuckerberg in or around 2003 and 2004.

12. Native files also can include other non-visible data that can bear on authenticity, such as Track Changes information that reveal a document's editing history or recent deletions from the document that can be forensically reconstructed. Such information is necessary to fully understand the provenance and modification of documents and is among the typical artifacts considered in an e-forgery investigation. Such relevant embedded metadata often is stripped out of a native document when it is rendered into a .tiff image or .pdf file, making production of the native version critical.

B. Information Available from Computers and Electronic Media Generally

13. While some information relevant to authenticity can be extracted from individual files, much more such information is available from an inspection of all of the computers or electronic media on which the files were created, viewed, stored, or modified. Critical information relating to backdating or e-forgery can be gleaned from a computer's file system; a computer's application, security, and event logs; the metadata on unrelated files; and the

unallocated space of digital media, including a computer's hard drive, to name just a few locations.

14. Even where documents were created on another computer, an inspection of computers or digital media on which a person simply opened, viewed, or saved the documents can provide significant information about the authenticity of those documents. This is because the mere act of opening a document on a computer can create a cached version of that document on the computer's hard drive. In e-forgery matters, I have sometimes found cached versions of a document that are inconsistent with the proponent's view of the authenticity.

15. Full inspection of each computer is accomplished first by performing a digital forensic copying (or imaging) of the computer's hard drive or hard drives and other digital media used with that computer. This is an entirely passive process and does not change any of the data on the drive or media. Digital forensic examiners perform their analyses from these digital forensic images, not the originals. A typical imaging of a laptop or desktop computer, or an external hard drive, takes between one and several hours. Once the digital forensic imaging process is complete, the computers can be returned to the owners for resumed usage.

16. For the reasons set forth above, it is critical to Stroz Friedberg's analysis of the authenticity of the Purported Contract and the Purported Emails that Stroz Friedberg create: (a) forensically-sound copies of all native electronic versions of the Purported Contract and the Purported Emails; and (b) forensically-sound copies of all computers and electronic media within Mr. Ceglia's possession, custody, or control, including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies.

A Possible Protocol for Digital Forensic Analysis

17. Typically, when the proponent of the authenticity of a document, such as Mr. Ceglia, is producing his computers and electronic media for inspection, Stroz Friedberg utilizes a protocol to protect private or privileged information. That protocol allows the digital forensic examiner to look at and rely on any information on the computers in conducting his or her authenticity examination. However, to protect private or privileged materials, the descriptions of such files or text should be redacted or masked in Stroz Friedberg's report. To accomplish this, in advance of writing the report or communicating with its client, Stroz Friedberg tenders to counsel for the owner of the computers ("Opposing Counsel") all file names, strings, fragments, and text that it intends to rely on in its report on authenticity. Opposing Counsel then can interpose an objection if any such file names, strings, fragments, or text from the computers are private or privileged. For any material objected to by Opposing Counsel, Stroz Friedberg uses a protocol to redact the content while still relying on the important metadata or other attributes.

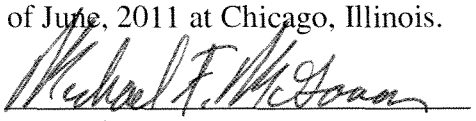
18. In addition, Stroz Friedberg's protocols incorporate a strict non-disclosure agreement to prevent it from disclosing, outside of its report, information from the computers. In sensitive cases, Stroz Friedberg even has conducted our examination at Opposing Counsel's offices, and under the supervision of Opposing Counsel's digital forensic expert, so that Stroz Friedberg does not ever have possession of the opposing party's digital forensic images and so that the opposing expert can verify that there is no inappropriate copying of data by Stroz Friedberg. Indeed, Stroz Friedberg's protocols normally require that the computers used for the inspection have no access to the Internet. As further protection, the digital forensic images can be secured in a media safe in a separately keyed room in between inspection sessions and only removed from the safe in the presence of both parties.

Conclusion

19. Stroz Friedberg should create: (a) forensically-sound copies of all native electronic versions of the Purported Contract and the Purported Emails; and (b) forensically-sound copies of all computers and electronic media within Mr. Ceglia's possession or control,

including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies. In addition, Stroz Friedberg should be allowed to fully analyze these forensically-sound copies.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 1st day of June, 2011 at Chicago, Illinois.



Michael F. McGowan