The Lack of Foundation Fosters Fraud

Federal Rules of Evidence
And
Electronic Evidence

By

O. Max Gardner III

The expanding market for that buying, selling and securitization of consumer debts has resulted in a serious problem regarding the "quality and admissibility" of the computer data that is being tendered to the United States Bankruptcy Courts to prove the nature and extent of consumer debt obligations. The same thing can be said with respect to the quality of the evidence that is being offered by Mortgage Servicers with respect to the nature and extent of the mortgage obligations of consumer homeowners. The analysis of these records by the attorneys for the debtors and by the Court has tended to overlook the underlying evidentiary foundations necessary to authenticate the same in order to create admissible and competent evidence. Also, since me of these records are generated in the normal course of business of an entity other than the proponent of the data in court, the business record foundation has also been either ignored or overlooked by the litigants and the courts. These are all important concepts in a consumer bankruptcy practice since the evidence presented in a proof of claim and in support of motion for relief from stay normally consist exclusively of "electronic evidence."

In order to introduce electronic records into evidence, the witness for the moving party must be able to establish all of the evidentiary foundations.

Fed. R. Evid. 104. The Judge acts as gatekeeper on the preliminary questions regarding the admissibility of evidence if a Federal Proceeding. The basic elements for the introduction of business records under the hearsay exception for records of regularly conducted activity all apply to records maintained electronically. *American Express v Vee Vinhnee, 205 Bankr. Lexis 2602 (BAP., 9th Cir. 2005)*.

Generally, such records must be:

1. Made at or near the time by, or from information transmitted by, a person with knowledge;

2. Made pursuant to regular practices of the business activity;

3. Kept in the course of regularly conducted business activity; and

4. The source, method, or circumstances of preparation must not indicate a lack of trustworthiness.

See Fed. R. Evid. 803(6) and United States v Catabran, 836 F.2d 453, 457 (9th Cir. 1988).

These elements must either be established by the testimony of the custodian or other qualified witness or must meet prescribed certification requirements. *Fed. R. Evid. 803(6)*. Such records, however, will not be admitted unless the court is also persuaded by their proponent that they are authentic. Ordinarily, because the business records foundation commonly covers the ground, the authenticity analysis is merged into the business record analysis without form focus on the question. *See 5 Weinstein 900.06[2][a]*. The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created.

Authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained: one must demonstrate that the record has been retrieved from the file, be it paper or electronic, and is the same as the record that was originally placed into the file. *Fed. R. Evid. 901(a)*. Footnote 5 to this Rule provides that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

Hence, the focus is not on the circumstances of the creation of the cord, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.

In the case of a paper record, the inquiry is into the procedures under which the file is maintained, including custody, access, and procedures for assuring that the records in the files are not tampered with. The foundation is well

understood and usually is easily established. *See Edward J. Imwinkelried, Evidentiary Foundations 4.03[a] (5th ed. 2002); 5 Weinstein 900.07[1][b][i]*.

The paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than the paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be.

The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled is all important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

There is really little mystery to all of these rules. All of these questions are recognizable as analogous to similar questions that may be asked regarding paper files: policy and procedures for access and for making corrections, as well as the risk of tampering. But the increasing complexity of ever-developing computer technology necessitates a more precise focus on the problem.

Some of these computer-related questions are becoming more important as the technology advances. For example, digital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to assure the continuing integrity of the records. *See George L. Paul, The "Authenticity Crisis" in Real Evidence, 15 PRAC. Litigator No. 6, at 45-49 (2004)*. This adds as extra dimension to consideration of whether the computer was "regularly tested" for errors. *See 5 Weinstein 901.11[2] (2005)*.

This ever-expanding complexity of the cyber world has prompted authors of the current version of the Manual for Complex Litigation to note that a judge should "consider the accuracy and reliability of computerized evidence" and that a "proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy." *Manual for Complex Litigation (Fourth), 11.446 (2004)*. The Manual quotes with approval the following statement for an Article by Gregory P. Joseph, *A Simplified Approach to Computer-Generated Evidence and Animations, 43 N.Y. Sch. L. Rev. 875(1999-2000)*. In the Article, it is stated that in general the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. "Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment

malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling." *Manual for Complex Litigation, Id, at fn. 6*.

In effect, it is becoming clearly recognized that early versions of computer foundations were too cursory, even thought the basic elements covered the ground. For example, it has been said that a qualified witness must testify as to the mode of the record preparation, that the computer is the standard acceptable type, and that business is conducted in reliance upon the accuracy of the computer in retaining and retrieving information. *Barry Russell, Bankruptcy Evidence Manual P803.17 (2005)*. These several elements, however, subsume a number of constituent elements.

Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. *Fed. R. Evid. 901(b)(9)*. Advisory Committee Note 7 to this Rule provides and "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."

Indeed, judicial notice is commonly taken of the validity of the theory underlying computers and of their general reliability. *Imwinkelried, Id., at 4.03[2].* Theory and general reliability, however, represent only part of the foundation. Professor Imwinkelried perceives electronic records as a form of scientific evidence and discerns an eleven-step foundation for the admissible of such records:

1. The business regularly uses a computer.

2. The computer is reliable.

3. The business has developed a procedure for inserting data into the computer.

4. The procedure has built-in safeguards to ensure accuracy and identify errors.

5. The business keeps the computer in a good state of repair and has regular and professional maintenance.

6. The computer system has appropriate firewalls and security features in order to eliminate the possibility of corruption or manipulation of data.

7. The witness had the computer readout certain data.

8. The witness used the proper procedures to obtain the readout including the entry of a proper username and password and the proper commands.

9. The computer was in proper working order at the time the witness obtained the readout.

10. The witness recognizes the exhibit as the readout.

11. The witness explains how he or she recognizes the readout.

12. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols and terms for the trier of fact.

13. The business has implemented a proper computer policy and system control procedures that limit access to the data.

14. The computer system can generate reports as to when any original data was changed, modified, or deleted, including the time and date, the name of the employee taking such action, and the basis for the action.

15. The business exercises control over access to the database.

16. The software programs have been verified for accuracy and all patches, fixes, and new features have been and are uploaded on a regular basis.

17. The business has implemented regular audit procedures to assure the continuing integrity of the records.

18. The business has a regular system to backup all databases and checks the system for accuracy on a daily basis.

19. The witness has complete access to the computer system and database, is familiar with how the data is entered, stored and maintained, has personal knowledge of ally verification and security systems, and can testify that all of these matters were personally verified in connection with the evidence proffered.

20. The witness must be able to offer evidence of sufficient training, experience and expertise in these areas to offer the detailed foundation evidence required for authentication.

How should the attorney for the Debtor deal with this type of evidence? It is suggested that a Motion to Strike the Affidavit with the defective account data should be filed. This type of motion can be filed pursuant to Rule 7012 of the Bankruptcy Rules and Rule 12(e) of the Federal Rules of Civil Procedure. The motion must be filed with "20 days after service" of the

Affidavit and the substantive objection is that the document is replete with data or account information that is not admissible and therefore immaterial to the issues before the Court.

O. Max Gardner III
403 South Washington Street
PO Box 1000
Shelby NC 28151-1000
704.487.0616 (v)
704.487.0619 (f)
maxgardner@maxgardner.com
http://www.maxgardnerlaw.com