Refining the Standard: Authenticating Computer-Based Evidence

M. Sean Fosmire is a shareholder in the Michigan law firm of Garan Lucow Miller, P.C., based in the firm's Marquette office.

Published July 15, 2006

Lawyers, judges, and writers on evidence have not paid much attention to the special issues of authentication that arise when a party seeks to introduce computer-based information into evidence. The few courts and authors that have mentioned those issues have usually cited Evidentiary Foundations, by Prof. Edward Imwinkelried of the University of Chicago, probably because he seems to be the only textbook author who has addressed the issue at all. See, for example, Conrad J. Jacoby, Defining A Standard for Admitting Electronic Evidence at Trial, published at LLRX on February 15, 2006, and David F. Axelrod, Are More Stringent Rules for Authenticating Electronic Records Coming?, published in the Business Crimes Bulletin in June 2006. Both articles discuss the ruling of a bankruptcy appellate panel based in California in the case *In re: Vinhnee*, 2005 WL 3609376 (B.A.P. 9th Cir. Dec. 16, 2005).

The issue in the *Vinhee* case was not whether the proper foundation had been laid under the business records exception to the hearsay rule. Rather, the panel noted, the issue was the more basic one of authentication of the data itself – showing that the data properly represented what it was claimed to show. The panel stated:

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

The panel cited the 5th edition of Prof. Imwinkelried's treatise at section 4.03[2], where he lists eleven foundational points that should be established in order to authenticate electronic evidence:

1. The business 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.
6. The witness had the computer readout certain data.

7. The witness used the proper procedures to obtain the readout.

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

9. The witness recognizes the exhibit as the readout.

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

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

It is my view that the professor's list is somewhat out of date – it seems quaint today to suggest that the attorney establish that "the business uses a computer", and the reference to "inserting data into the computer" sounds a little elementary. Indeed, some of the points that are listed do not reflect much familiarity with the operation of computers in everyday business use and the way in which inaccuracies can find their way into computer-based data. It is not clear, for example, what is accomplished by establishing that "the computer is reliable". In most cases, though of course not all, a computer which is not "reliable" will be taken out of service and replaced.

Similarly, it seems unnecessary to establish that the computer was "in working order" at the time the report was produced. A computer which is not "in working order" will not insinuate bogus data into a compilation – it simply will not work, and thus will not produce any report. If corrupted data is introduced into the system, this will usually be readily apparent because the data will not display or print at all, or it will display unintelligible characters. It would be extremely unusual for data corruption to do nothing but change the values of numbers. By contrast, errors in data input or in data retrieval can very easily give rise to inaccurate entries.

The Federal Judicial Center's Manual for Complex Litigation, 4th Edition, briefly addresses evidentiary issues at §11.447, p. 82, and fairly summarizes the potential authentication problems that arise when computer-based evidence is offered:

> "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."

Although the Manual cautions the judge that he or she should therefore "consider the accuracy and reliability of computerized evidence", it does not provide any detail about the requirements that should be imposed, or the factors to consider, to lay the foundation for admission of that evidence.

Updating the standard

Authentication issues, of course, are addressed under Rule 901, which begins with a general principle:

> Rule 901. Requirement of Authentication or Identification
>
> (a) General provision. 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.

Section (b) of the rule then goes on to provide a series of illustrations, examples of methods of authenticating offered evidence, which are expressly stated to be provided "by way of illustration only, and not by way of limitation". This rule, perhaps more than any of the other rules of evidence, clearly is intended to give primacy to the discretion of the trial judge on the question of what is, in fact "evidence sufficient to support a finding that the matter in question is what its proponent claims". One of the several illustrations is particularly pertinent to electronic evidence:

(9) Process or system – Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

I believe that Prof. Imwinkelried's list can be updated and enhanced to with the following list of foundational questions. Some of these items will of course not be relevant at all as to certain items of electronic evidence. This list is intended to be comprehensive as to the matters that may be established by counsel; requiring proof of each and every one of these items would perhaps be regarded as "overkill" in a particular case. Note that, absent an agreement from opposing counsel, it may be necessary to offer the testimony of a company's IT person as well as testimony from the person who generated or secured the item offered into evidence.

1. Establish the date that the computer system was put into place, and that it is maintained and serviced on a regular basis.

2. Establish what security routines are used to safeguard the data on the system. Who has access to input terminals, and who has access to be able to produce reports? What login procedures are used to ensure that only authorized personnel are able to use the system? How are login passwords safeguarded? (A user who writes her password on her computer monitor for ease of reference – it did happen – is not a security-minded user.)

3. Establish that there is a firewall, regularly maintained, monitored, and updated, which prevents outsiders from surreptitiously gaining access to the system.

4. Identify the software which is used and the version. When did the business adopt the software, and when did the current version go into service? How widely used is the software in the company's line of business?

5. Establish the way the software works in general. Does it require a separate user login? What information is entered, how is it stored, and how is it retrieved?

6. Identify how many employees use the software, and describe how they have been trained in its use.

7. Describe who enters the data, where it comes from, and how it is entered. Identify any categories or other assignments that are attached to the separate items of data, and how the decision is made to assign them.

8. Identify any procedures that the software uses to catch recognizable errors and to bring them to the attention of the input operator. Identify any continuous or random quality checks that are used to ensure that information is correctly entered and that categories and other parameters are accurately assigned.

9. If the program in question produces separate files for each entry or item produced, identify the pertinent system information for the file – date of creation, date last modified, date last accessed. (A word processing document that was created on May 1, 2005 but was last modified two days before trial may have lost its credibility.)

10. Explain any apparent discrepancies between the paper version that is produced and the original electronic item. (Documents produced with a word processor often use a date code that is automatically updated, and a document that was created on May 1, 2005 but was printed for use as an exhibit two days before trial will display the wrong date. Go back to the filestamp information to verify the date of last modification.)

11. Identify the means by which regular reports are done or retrieval of data is done for the company's day-to-day business purposes. Are the reports electronic only or are there paper copies made? What is done with the reports? Who reads or reviews them, and for what purpose? (Review of reports by management is a common way that inadvertent errors are

caught and corrected.)

12. Explain how the choices were made to produce the particular report that is now being offered. Which categories or parameters were used, and which records was the software requested to retrieve and display? Which filters were used, and why? How was the software instructed to sort the resulting entries? What requests for other display parameters were entered?

13. Establish that the witness recognizes the report as the results of the request, and explains how he or she recognizes it. (The witness should be the person who produced the report.)

14. Establish that the witness is familiar with all entries, terms, categories, filters, sorting instructions, etc., used to create the report, and can explain how and why they were applied to produce the report in question.

15. If either the printed report or the source electronic file contains special symbols, terms, commands, or formulas, ask the witness to explain the meaning of these items. A witness discussing a spreadsheet, for example, should be prepared to identify the formulas used and how they are created and used to perform calculations on the figures in the spreadsheet. The ranges that are referenced in the formulas should have been inspected to ensure that they were properly defined.

16. If the offered item is a summary report of selected entries from the electronic data, counsel for the proponent of the report should also prepare and make available for review by counsel and by the court – but not for introduction as evidence – a complete report showing all entries for the period of time in question, for purposes of comparison with the special selection report that is being offered. That complete report, as well as copies of the original data files from which the report was created, should have been prepared and made available to opposing counsel for review well in advance of the trial or hearing at which the report is offered into evidence.

The last-noted point can best be understood by use of an example. Consider a company employing 35 people and which uses QuickBooks to enter receipts, write checks, and issue invoices to customers. The company's attorney wants to establish that a total of $44,500 in checks was issued by the company to pay taxes in 2005. The report that is offered is produced by requesting QuickBooks to prepare a summary report listing all checks issued by the company, filtered for the date range 1-1-05 to 12-31-05 and for the assigned category of "Taxes", and the attorney wants to offer that summary report into evidence.

The information residing within the QuickBooks data files is thought to be accurate, and the company relies on that presumption of accuracy, but mistakes are possible. As data is entered, some errors in transcription may creep in. If a dyslexic operator entered "tasex" instead of "taxes" for one item, or if a forgetful operator simply forgot to enter a category for that item, a search based on the category "taxes" will not catch it.

One way to double-check to ensure that an error like this has not been made, and to establish that fact to the satisfaction of the court, would be to run and make available a separate full report showing all items in all categories for the year 2005, sorted by category. In this way, an item assigned to an erroneous category or simply lacking a category assignment would appear on the full list and the error would be caught.

After authentication: Which rule to use?

Most attorneys simply assume that electronic records will meet the criteria for an exception to the hearsay rule as business records. The electronic records themselves would so qualify in most cases, but at the time of trial it is usually necessary to produce something on paper, something that can be held in the hand, something that the jury can examine in the course of deliberations. That paper exhibit itself, however, may not qualify as a business record.

The evidence rules still have an imperfect fit with business records maintained in electronic format. There is no one rule that has been specifically drafted to address the conversion of electronic data to paper or other formats for use at trial.

A report such as the one cited in the example could qualify as a "summary" of voluminous data, and as such can be offered under Rule 1006 of the Federal Rules of Evidence. A summary under Rule 1006 does not have to summarize all of the data; a summary or calculation of the selections relevant to the issue at hand would qualify. If the report was specially made for the trial, and is not one which is routinely prepared under the company's normal business practices, it would arguably not qualify as a business record, and thus qualifying it as a summary under Rule 1006 would be the only proper means of admitting it.

Rule 1006 allows the proponent to offer a summary if the entirety of the data would be too voluminous or too over-inclusive to be conveniently examined in court. Admissibility under this rule is subject to the following special conditions:

- The originals, or duplicates of the originals, shall be made available to the other parties for examination or copying, or both, at a reasonable time and place.

- The court may order that they be produced in court.

The questions listed above, particularly item 12, were designed to include the steps needed to establish that the summary was properly constructed to limit the summary report to relevant information, and the points mentioned in the last item – creating the special report and making the data files available to opposing counsel – come as close as possible, given the particular characteristics of electronic data, to the rule's requirement that the "originals" on which the summary is based be made available to the opposition for examination and comparison with the summary report. Rule 1006 requires that the proponent make the original information available for inspection by other counsel at a reasonable time and place. Several courts have held that this means that they must be available in advance of the hearing or trial at which the summary is offered, and they have also ruled that that obligation is independent of the discovery process and thus does not depend on a request made by the opponent. See *Air Safety, Inc. v. Roman Catholic Archbishop of Boston*, 94 F.3d 1 (1st Cir. 1996); *U.S. v. Bertoli*, 854 F. Supp. 975 (D.N.J. 1994), *aff'd in part, vacated in part on other grounds* 40 F.3d 1384 (3d Cir. 1994).

The precise questions to be asked and the precise nature of the corroborating offer of proof will depend upon the software in question. An attorney who is familiar with the operation of the software will be able to determine what must be shown in order to provide the additional foundational assurance needed to allow the court to decide that the requirement of authentication has been met – or to determine that it should be challenged. Indeed, such familiarity may be required. Some courts have held that the inability of counsel to explain the meaning of the contents of a summary report to the satisfaction of the court justifies a refusal to admit it into evidence. *Vasey v. Martin Marietta Corp*., 29 F.3d 1460 (10th Cir. 1994).

The rules of evidence are based upon many years of experience by attorneys and the courts, and they are always being updated to reflect their new experiences. With the widespread adoption of computer technology in ordinary business over the last decade, that experience has undergone dramatic changes, a fact which has led to the pending amendments of the Federal Rules of Civil Procedure (expected to be effective December 1, 2006), the first such amendment since 2000.

Data that are maintained in electronic format are becoming a common subject of evidentiary disputes, frequently displacing the traditional evidentiary issues over paper documents. This is underscored by the fact that virtually all paper documents produced today start out in electronic format. Lawyers must keep themselves apprised of how electronic information is created, stored, maintained, secured, and retrieved by their clients in the course of their business operations, if they want to ensure that the crucial item that they need to introduce will be accepted by the courts as admissible evidence in support of their clients' case at the time of trial.

BACK TO TOP OF PAGE

[LLRX Front Page | Bookstore | Archives | About LLRX | Subscribe |
| Comments | Linking | Privacy Policy]