Proskauer

New Rules Tackle Authentication of Electronic Data

Minding Your Business Blog on **December 5, 2017**

On December 1, 2017, two amendments to the Federal Rules of Evidence came into effect that impact how courts authenticate digital evidence. The addition of two categories to Rule 902's list of self-authenticating documents seeks to streamline the introduction of digital evidence by avoiding costly delays that often serve little purpose. In doing so, it promises greater efficiency to those who adapt their practices to the new requirements.

Rule 902(13) waives the requirement of external authentication for "records generated by an electronic process or system," provided that the accuracy of the process or system is certified by a person who meets the qualification requirements of 902(11) or (12). Examples of such records provided by the Advisory Committee include an operating system's automated log of all USB devices connected to the computer, or a phone software's machine-generated record of the time, date, and GPS coordinates of each picture taken.

Rule 902(14) provides that "certified data copied from an electronic device, storage medium, or file" will likewise be self-authenticating, again on the condition that such data is certified by a person qualified according to the standard of 902(11) or (12). This rule relies on documents' digital fingerprints that can be matched to confirm that a copy is identical to the original.

In proposing the amendments, the Advisory Committee pointed to the fact that evidence of the type covered by 902(13) and (14) was rarely the subject of a legitimate authenticity dispute; more often, a party would wait until its opponent had incurred the expense and inconvenience of producing an authentication expert before either stipulating to authenticity, or failing to challenge the authentication testimony presented. By drawing on the procedures in place for business records and allowing authentication based on certification, the new rules "essentially leave the burden of going forward on authenticity questions to the opponent of the evidence."

The amendments point to a number of best practices that parties should adopt in order to take advantage of the simplified authentication process for electronic information. Firstly, a specialist should be retained who can testify to the accuracy of the electronic process (in the case of 902(13)) or to the identity of digital fingerprints for the documents in question (in the case of 902(14)). In addition, both provisions specify the format of the information that is covered: 902(13) requires records generated by an automated process (not, for example, information manually entered by an individual), while 902(14) encompasses only files that are exact duplicates of each other, and would therefore exclude a document whose format had been changed (for example, from a word to an image document). It is therefore vital to implement file collection, transfer, and storage policies that ensure the relevant data is preserved.

The new rules represent a significant change in how electronic evidence is treated. For parties that take appropriate measures, however, they promise to save time and resources, and promote greater certainty.

View Original