

# O'NEILL & BORGES

ATTORNEYS AT LAW

AMERICAN INTERNATIONAL PLAZA  
250 MUÑOZ RIVERA AVE, SUITE 800  
SAN JUAN, PUERTO RICO 00918-1813

TEL (787) 764-8181  
FAX (787) 753-8944  
WWW.ONEILLBORGES.COM

## LITIGATION DEPARTMENT NEWSLETTER

DECEMBER 2009

### THE NEW PUERTO RICO RULES OF EVIDENCE AND HOW THEY MAY IMPACT YOUR BUSINESS OPERATION

#### Key Changes

The amended Puerto Rico Rules of Evidence will come into effect on January 1st, 2010. They codify new privileges and explicitly provide for the discovery and authentication of electronically-stored information. The following are among the most important amendments that may impact how companies run their businesses and manage legal conflicts:

- **Rule 406** establishes that a corporation's routine practices may be used as evidence of habit. A habit or routine practice may be evidenced through testimony or other demonstration of a particular number of specific acts.
- **Rule 901(B)** now provides specific examples for the authentication process for electronically stored information.

#### Authentication of Electronic Evidence

Authentication is required for the admissibility of evidence. Specifically, in order to be able to have evidence easily and cost-efficiently admitted into evidence, the party offering an item of non-testimonial evidence should have in place business practices that help to readily prove that the item is what the party "claims it to be." As to electronic data, the new Rules of Evidence specifically provide the following:

- **Rule 901(B)(5)** now deems a data compilation to be a form of "ancient

document" generally presumed to be self-authenticating.

- **Rule 901(B)(12)** provides that a system or process may be authenticated by describing the process or system used to obtain a result and demonstrating that the process or system normally generates accurate results.
- **Rule 901(B)(13)** provides that an electronic record may be authenticated by proving the integrity of the system used to store the record. Integrity may be demonstrated through evidence of the system's proper operation or, in case of malfunction, by showing that the malfunction did not affect the record's integrity.
- **Rule 901(B)(14)** provides that electronic mail may be authenticated through evidence of the integrity of the system through which the message was created, sent or received.
- **Rule 902(E)** acknowledges that a data compilation may be a form of public record for purposes of self-authentication.
- **Rule 902(L)** establishes a presumption in favor of an electronic record's integrity if supported by a sworn statement showing that: (i) the record was stored by a party adverse to that which offers it as evidence or (ii) it was created in the ordinary course of business by a person that is not a party

to the proceedings and when storing the information, such non-party did not act under the control of the party that offers it as evidence.

### Impact on business operations

Although it is difficult to predict the new Rules' full impact on business practices, we note:

□ An adequate and accurate administration of a business's information technology system is essential. Proper storage and management of electronic data –as a routine business practice— may be important in gauging the usefulness of such data in a later civil proceeding. Specifically, it may make it easier and less-costly to prove in court that the data is what it appears to be.

□ A “systems administrator” may facilitate the procedure of authenticating a process or system, as well as the information retrieved through a particular process or system. This employee's or contractor's role in a potential litigation should be considered carefully.

□ Where substantial electronic data is particularly important to a business operation, having a business record that can be characterized as a “data compilation” may prove particularly useful. Not only will that data compilation allow you to control such process while in progress, the compilation itself, *i.e.* the report generated by the particular program at issue, should be deemed self-authenticating and more readily admissible as evidence should a claim arise.

□ Maintain an accurate record of system malfunctions. This facilitates ascertaining the integrity of a particular record or explaining whether a malfunction tainted the evidence. Having such records, for example, will assist in proving that a particular e-mail was never received or that it was received later than when it was sent.

□ Implement an electronic information policy in your business. Written storage practices may constitute evidence of habit. Consequently, a well-established policy for the management of electronic information prior to any legal controversy may help demonstrate a habit as to the handling of electronic data.

For more information in Spanish regarding the key changes to the Rules of Evidence, you may check <http://www.ramajudicial.pr/sistema/supremo/conferencia.htm#>.

XXXXXXXXXXXXXXXXXXXX

*Because of the general nature of this newsletter, its contents should not be considered as legal advice or a legal opinion. The impact of other regulatory record retention obligations upon a particular business is also beyond the scope of this newsletter. For further information and assistance in connection with these matters, please contact our firm's Litigation Department.*

XXXXXXXXXXXXXXXXXXXX

Litigation Department Partners	
Hermann D. Bauer-Alvarez	Mauricio O. Muñiz Luciano
Shylene J. De Jesús	Alfredo F. Ramírez-MacDonald
Mariacté Correa-Cestero	David Rivé-Power
Christian M. Echavarrri-Junco	Antonio L. Roig-Lorenzo
David P. Freedman	Jorge A. Rullán
Carla García-Benitez	Salvador J. Antonetti-Stutts
Luis C. Marini Biaggi	Carlos A. Valldejuly-Sastre
Associates	
Nynorsha Lugo-Sánchez	Liza Ríos
Mario A. Arroyo-Maymí	Ariel Rivera
Ubaldo Fernández	Sharlene Malavé
Nashely Pagán-Isona	Lourdes Arroyo-Portela
Maria Celeste Colberg	Ana Margarita Rodríguez
Luis S. Herrero	Carlos Sagardía