SUPREME COURT OF PENNSYLVANIA
COMMITTEE ON RULES OF EVIDENCE

NOTICE OF PROPOSED RULEMAKING

Proposed Adoption of Pa.R.E. 902(13) & Pa.R.E. 902(14)

The Committee on Rules of Evidence propose the adoption of Pennsylvania Rule of Evidence 902(13) and 902(14) concerning the self-authentication of certified records generated by an electronic process or system and certified data copied from an electronic device, storage medium, or file, for the reasons set forth in the accompanying explanatory report. Pursuant to Pa.R.J.A. No. 103(a)(1), the proposal is being published in the *Pennsylvania Bulletin* for comments, suggestions, or objections prior to submission to the Supreme Court.

Any reports, notes, or comments in the proposal have been inserted by the Committee for the convenience of those using the rules. They neither will constitute a part of the rules nor will be officially adopted by the Supreme Court.

Additions to the text of the proposal are bolded and underlined; deletions to the text are bolded and bracketed.

The Committee invites all interested persons to submit comments, suggestions, or objections in writing to:

Daniel A. Durst, Counsel
Committee on Rules of Evidence
Supreme Court of Pennsylvania
Pennsylvania Judicial Center
PO Box 62635
Harrisburg, PA 17106-2635
FAX: 717.231.9536
evidencerules@pacourts.us

All communications in reference to the proposal should be received by **February 22, 2019.** E-mail is the preferred method for submitting comments, suggestions, or objections; any e-mailed submission need not be reproduced and resubmitted via mail. The Committee will acknowledge receipt of all submissions.

By the Committee on Rules of Evidence,

John P. Krill, Jr.
Chair

SUPREME COURT OF PENNSYLVANIA
COMMITTEE ON RULES OF EVIDENCE

REPORT

Proposed Adoption of Pa.R.E. 902(13) & Pa.R.E. 902(14)

The Committee on Rules of Evidence is considering proposing the adoption of Pennsylvania Rule of Evidence 902(13) and 902(14) concerning the self-authentication of certified records generated by an electronic process or system and certified data copied from an electronic device, storage medium, or file.

The Federal Advisory Committee on Evidence considered the expense and inconvenience of producing a witness to authenticate an item of electronic evidence given that the adversary often either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. In light of business records able to be self-authenticated by certification, see F.R.E. 902(11) & (12), the Advisory Committee proposed rule amendments in 2015 that would provide for a similar procedure where the parties can determine in advance of trial whether a real challenge to authenticity will be made to electronic evidence, and can then plan accordingly.

As approved by the Rules Committee of the Judicial Conference, F.R.E. 902(13) & (14) were adopted, effective December 1, 2017. Specifically, F.R.E. 902(13) states:

> **Certified Records Generated by an Electronic Process or System.** A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

To establish authenticity under this Rule, the proponent must present a certification containing information that would be sufficient to establish authenticity if that information was provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

Illustrations of how F.R.E. 902(13) can be used include:

> **1. Proving that a USB device was connected to (*i.e.*, plugged into) a computer:** In a hypothetical civil or criminal case in Chicago, a disputed

issue is whether Devera Hall used her computer to access files stored on a USB thumb drive owned by a co-worker. Ms. Hall's computer uses the Windows operating system, which automatically records information about every USB device connected to her computer in a database known as the "Windows registry." The Windows registry database is maintained on the computer by the Windows operating system in order to facilitate the computer's operations. A forensic technician, located in Dallas, Texas, has provided a printout from the Windows registry that indicates that a USB thumb drive, identified by manufacturer, model, and serial number, was last connected to Ms. Hall's computer at a specific date and time.

Without Rule 902(13): Without Rule 902(13), the proponent of the evidence would need to call the forensic technician who obtained the printout as a witness, in order to establish the authenticity of the evidence. During his or her testimony, the forensic technician would typically be asked to testify about his or her background and qualifications; the process by which digital forensic examinations are conducted in general; the steps taken by the forensic technician during the examination of Ms. Hall's computer in particular; the process by which the Windows operating system maintains information in the Windows registry, including information about USB devices connected to the computer; and the steps taken by the forensic examiner to examine the Windows registry and to produce the printout identifying the USB device.

Impact of Rule 902(13): With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer; that the process by which such information is recorded produces an accurate result; and that the printout accurately reflected information stored in the Windows registry of Ms. Hall's computer. The proponent would be required to provide reasonable written notice of its intent to offer the printout as an exhibit and to make the written certification and proposed exhibit available for inspection. If the opposing party did not dispute the accuracy or reliability of the process that produced the exhibit, the proponent would not need to call the forensic technician as a witness to establish the authenticity of the exhibit. (There are many other examples of the same types of machine-generated information on computers, for example, Internet browser histories and Wi-Fi access logs.)

...

3. Proving that a person was or was not near the scene of an event: Hypothetically, Robert Jackson is a defendant in a civil (or criminal) action alleging that he was the driver in a hit-and-run collision with a U.S. Postal Service mail carrier in Atlanta at 2:15 p.m. on March 6, 2015. Mr. Jackson owns an iPhone, which has software that records machine-generated dates, times, and GPS coordinates of each picture he takes with his iPhone. Mr. Jackson's iPhone contains two pictures of his home in an Atlanta suburb at about 1 p.m. on March 6. He wants to introduce into evidence the photos together with the metadata, including the date, time, and GPS coordinates, recovered forensically from his iPhone to corroborate his alibi that he was at home several miles from the scene at the time of the collision.

Without Rule 902(13): The proponent would have to call the forensic technician to testify about Mr. Jackson's iPhone's operating system; his search of the phone; how the metadata was created and stored with each photograph; and that the exhibit is an accurate record of the photographs.

With Rule 902(13): The proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibits and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the iPhone's logs, then the proponent would not have to call the technician to establish authenticity.

Hon. Paul W. Grimm *et. al.*, *Authenticating Digital Evidence*, 69 Baylor L. Rev. 1, 42-44 (2017).

F.R.E. 902(9) states:

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

This Rule sets forth a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, other than through the testimony of a foundation witness. A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity if that information was provided by a witness at trial. If the certification

provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.

The Committee considered whether adoption of rules similar to the new Federal Rules would be consistent with purpose of the Pennsylvania Rules of Evidence "to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination." Pa.R.E. 102. At the risk of oversimplification, the Committee notes that the Federal Rules do not alter the requirement of authentication; they merely permit an out-of-court certification to replace in-court testimony.

Pursuant to Pa.R.E. 901(a), the proponent is required to produce sufficient extrinsic evidence to authenticate or attribute evidence as being what the proponent claims it to be. For example, when a proponent wishes to introduce a voice recording and connect the voice to a specific speaker, the proponent can have a witness familiar with the speaker's voice testify as to the witness's opinion whether the voice on the recording is that of the speaker. *See* Pa.R.E. 901(b)(5).

Likewise, if the proponent wishes to introduce evidence of a result of a process or system, then the proponent must introduce extrinsic evidence describing the process or system and show that it produces an accurate result. *See* Pa.R.E. 901(b)(9). For example, an x-ray, unlike a photograph or videotape, cannot be authenticated by the operator of the imaging equipment because the operator cannot accurately see what is being depicted on the x-ray. Hence, the x-ray can be authenticated pursuant to Rule 901(b)(9) through evidence regarding the capability of the imaging equipment, the operation of equipment, the training of the operators, and the accuracy and clarity of the resulting image. However, in current practice, seldom is authenticity challenged with long established, well-known, and understood processes or systems where results are generally accepted as accurate.

Rule 901(b)(9) also has application to computer generated records. *See, e.g., Wachovia Bank, N.A. v. Gemini Equipment Co.*, 2006 WL 5429543 (Dauphin Co. 2006). While Pennsylvania precedent is scant, F.R.E. 902(b)(6), the analogue to Pa.R.E. 901(b)(9), has been more definitively applied to computer output. *See* 5 Federal Evidence § 9:20 (4th ed.) (discussing application to, *inter alia*, computer output).

As reliance on electronic processes and systems increases, so does a sense of familiarity and trustworthiness that records generated by same are done so without the potential bias or error inherent when records are generated by human involvement. An accurate record generated by computation requires only an understanding of the computation process or system to be authenticated. Pa.R.E. 902(13) would permit this task to be accomplished by certification rather than live testimony.

Similarly, a comparison of a unique identifier produced by an algorithm (*i.e.*, hashtag) in the source data with the copied data can be used to authenticate the copied data as being identical to the source data. Pa.R.E. 902(14) allows the authentication to be accomplished by certification and without the need for extrinsic evidence.

Broadly stated, the use of certifications in lieu of testimony is not foreign concept in Pennsylvania. *See, e.g.*, Pa.R.Crim.P. 574 (permitting the admission of forensic lab reports by certification in lieu expert testimony). More specifically, the use of certifications in lieu of authentication testimony has long been acceptable by the Rules of Evidence and statute. *See* Pa.R.E. 902(4), (11), & (12); 42 Pa.C.S. § 6106 (self-authentication of documents filed in public offices).

Borrowing language largely from F.R.E. 902(13) and F.R.E. 902(14), together with their commentary, the Committee seeks comment about the utility of incorporating these provisions into the Pennsylvania Rules of Evidence.

ARTICLE IX. AUTHENTICATION AND IDENTIFICATION

* * *

Rule 902. Evidence That Is Self-Authenticating

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(1) Domestic Public Documents That Are Sealed and Signed. A document that bears:

(A) a seal purporting to be that of the United States; any state, district, commonwealth, territory, or insular possession of the United States; the former Panama Canal Zone; the Trust Territory of the Pacific Islands; a political subdivision of any of these entities; or a department, agency, or officer of any entity named above; and

(B) a signature purporting to be an execution or attestation.

(2) Domestic Public Documents That Are Not Sealed But Are Signed and Certified. A document that bears no seal if:

(A) it bears the signature of an officer or employee of an entity named in Rule 902(1)(A); and

(B) another public officer who has a seal and official duties within that same entity certifies under seal – or its equivalent – that the signer has the official capacity and that the signature is genuine.

(3) Foreign Public Documents. A document that purports to be signed or attested by a person who is authorized by a foreign country's law to do so. The document must be accompanied by a final certification that certifies the genuineness of the signature and official position of the signer or attester – or of any foreign official whose certificate of genuineness relates to the signature or attestation or is in a chain of certificates of genuineness relating to the signature or attestation. The certification may be made by a secretary of a United States embassy or legation; by a consul general, vice consul, or consular agent of the United States; or by a diplomatic or consular official of the foreign country assigned or accredited to the United States. If all parties have been given a reasonable opportunity to investigate the document's authenticity and accuracy, the court may for good cause, either:

(A) order that it be treated as presumptively authentic without final certification; or

(B) allow it to be evidenced by an attested summary with or without final certification.

(4) Certified Copies of Public Records. A copy of an official record – or a copy of a document that was recorded or filed in a public office as authorized by law– if the copy is certified as correct by:

(A) the custodian or another person authorized to make the certification; or

(B) a certificate that complies with Rule 902(1), (2), or (3), a statute or a rule prescribed by the Supreme Court.

(5) Official Publications. A book, pamphlet, or other publication purporting to be issued by a public authority.

(6) Newspapers and Periodicals. Material purporting to be a newspaper or periodical.

(7) Trade Inscriptions and the Like. An inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control.

(8) Acknowledged Documents. A document accompanied by a certificate of acknowledgment that is lawfully executed by a notary public or another officer who is authorized to take acknowledgments.

(9) Commercial Paper and Related Documents. Commercial paper, a signature on it, and related documents, to the extent allowed by general commercial law.

(10) Presumptions Authorized by Statute. A signature, document, or anything else that a statute declares to be presumptively or *prima facie* genuine or authentic.

(11) Certified Domestic Records of a Regularly Conducted Activity. The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with Pa.R.C.P. No. 76. Before the

trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record – and must make the record and certification available for inspection – so that the party has a fair opportunity to challenge them.

(12) **Certified Foreign Records of a Regularly Conducted Activity.** In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification rather than complying with a statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11).

(13) **Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).**

(14) **Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).**

(15) **Certificate of Non-Existence of a Public Record.** A certificate that a document was not recorded or filed in a public office as authorized by law if certified by the custodian or another person authorized to make the certificate.

Comment

This rule permits some evidence to be authenticated without extrinsic evidence of authentication or identification. In other words, the requirement that a proponent must present authentication or identification evidence as a condition precedent to admissibility, as provided by Pa.R.E. 901(a), is inapplicable to the evidence discussed in Pa.R.E. 902. The rationale for the rule is that, for the types of evidence covered by Pa.R.E. 902, the risk of forgery or deception is so small, and the likelihood of discovery of forgery or deception is so great, that the cost of presenting extrinsic evidence and the waste of court time is not justified. Of course, this rule does not preclude the opposing

party from contesting the authenticity of the evidence. In that situation, authenticity is to be resolved by the finder of fact.

Pa.R.E. 902(1), (2), (3), and (4) deal with self-authentication of various kinds of public documents and records. They are identical to F.R.E. 902(1), (2), (3), and (4), except that Pa.R.E. 901(4) eliminates the reference to Federal law. These paragraphs are consistent with Pennsylvania statutory law. *See, e.g.* 42 Pa.C.S. § 6103 (official records within the Commonwealth); 42 Pa.C.S. § 5328 (domestic records outside the Commonwealth and foreign records); 35 P.S. § 450.810 (vital statistics); 42 Pa.C.S. § 6106 (documents filed in a public office).

The admission of a self-authenticating record of a prior conviction also requires sufficient evidence, either direct or circumstantial, to prove that the subject of the record is the same person for whom the record is offered in a proceeding. *See, e.g., Commonwealth v. Boyd*, 344 A.2d 864 (Pa. 1975).

Pa.R.E. 902(5), (6) and (7) are identical to F.R.E. 902(5), (6), and (7). There are no corresponding statutory provisions in Pennsylvania; however, 45 Pa.C.S. § 506 (judicial notice of the contents of the Pennsylvania Code and the Pennsylvania Bulletin) is similar to Pa.R.E. 902(5).

Pa.R.E. 902(8) is identical to F.R.E. 902(8). It is consistent with Pennsylvania law. *See Sheaffer v. Baeringer*, 29 A.2d 697 (Pa. 1943); *Williamson v. Barrett*, 24 A.2d 546 (Pa. Super. 1942); 21 P.S. §§ 291.1-291.13 (Uniform Acknowledgement Act); 57 Pa.C.S. §§ 301-331 (Revised Uniform Law on Notarial Acts). An acknowledged document is a type of official record and the treatment of acknowledged documents is consistent with Pa.R.E. 902(1), (2), (3), and (4).

Pa.R.E. 902(9) is identical to F.R.E. 902(9). Pennsylvania law treats various kinds of commercial paper and documents as self-authenticating. *See, e.g.*, 13 Pa.C.S. § 3505 (evidence of dishonor of negotiable instruments).

Pa.R.E. 902(10) differs from F.R.E. 902(10) to eliminate the reference to Federal law and to make the paragraph conform to Pennsylvania law. In some Pennsylvania statutes, the self-authenticating nature of a document is expressed by language creating a "presumption" of authenticity. *See, e.g.,* 13 Pa.C.S. § 3505.

Pa.R.E. 902(11) and (12) permit the authentication of domestic and foreign records of regularly conducted activity by verification or certification. Pa.R.E. 902(11) is similar to F.R.E. 902(11). The language of Pa.R.E. 902(11) differs from F.R.E. 902(11) in that it refers to Pa.R.C.P. No. 76 rather than to Federal law. Pa.R.E. 902(12) differs from F.R.E. 902(12) in that it requires compliance with a Pennsylvania statute rather than a Federal statute.

Pa.R.E. 902(13) is identical to F.R.E. 902(13). This rule establishes a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. The rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

A certification under this rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds - including hearsay, relevance, or in criminal cases the right to confrontation. For example, a certification authenticating a computer output, such as a spreadsheet or a printout of a webpage, does not preclude an objection that the information produced is unreliable - the authentication establishes only that the output came from the computer.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(13) is solely limited to authentication of a record generated by an electronic process or system and any attempt to satisfy a hearsay exception must be made independently.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

Nothing in Rule 902(13) is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including though judicial notice where appropriate.

Pa.R.E. 902(14) is identical to F.R.E. 902(14). This rule establishes a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, using a certificate rather than through the testimony of a foundation witness. A proponent establishing authenticity under this rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record of the certifying person testified, then authenticity is not established under this rule.

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm

based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This Rule allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The Rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.

A certification under this rule can only establish that the proffered item is authentic. The opponent remains free to object to admissibility of the proffered item on other grounds - including hearsay, relevance, or in criminal cases the right to confrontation. For example, in a criminal case in which data copied from a hard drive is proffered, the defendant can still challenge hearsay found in the hard drive, and can still challenge whether the information on the hard drive was placed there by the defendant.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

Nothing in Rule 902(14) is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including though judicial notice where appropriate.

Pa.R.E. 902**[(13)]** **(15)** has no counterpart in the Federal Rules. This rule provides for the self-authentication of a certificate of the non-existence of a public record, as provided in Pa.R.E. 803(10)(A).

Note: Adopted May 8, 1998, effective October 1, 1998; amended November 2, 2001, effective January 1, 2002; amended February 23, 2004, effective May 1, 2004; rescinded and replaced January 17, 2013, effective March 18, 2013; amended November 7, 2016, effective January 1, 2017; amended June 12, 2017, effective November 1, 2017**; amended , 2018, effective , 2018**.

Committee Explanatory Reports:

Final Report explaining the November 2, 2001 amendments adding paragraphs (11) and (12) published with Court's Order at 31 Pa.B. 6384 (November 24, 2001). Final Report explaining the February 23, 2004 amendment of paragraph (12) published with Court's Order at 34 Pa.B. 1429 (March 13, 2004). Final Report explaining the January 17, 2013 rescission and replacement published with the Court's Order at 43 Pa.B. 651 (February 2, 2013). Final Report explaining the November 7, 2016 addition of paragraph (13) published with the Court's Order at 46 Pa.B. 7436 (November 26, 2016). Final Report explaining the June 12, 2017 amendment of the Comment published with the Court's Order at 47 Pa.B. **3491** (**June 24**, 2017). **Final Report explaining the , 2018 amendment of paragraphs (4), (6), and (12) published with the Court's Order at 48 Pa.B. (, 2018).**