The Fidelity Law Journal

published by
The Fidelity Law Association

Volume XXIV, November 2018

The Fidelity Law Journal

published by

The Fidelity Law Association

Volume XXIV, November 2018

Cite as XXIV FID. L.J. ___ (2018)

The Fidelity Law Journal is published annually. Additional copies may be purchased by writing to: The Fidelity Law Association, c/o Chiesa Shahinian & Giantomasi PC, One Boland Drive, West Orange, New Jersey 07052.

MODERNIZING LOAN FRAUD: THE PROLIFERATION AND EVOLUTION OF DIGITAL LOAN TRANSACTIONS

Scott L. Schmookler
Katherine Musbach[1]

I. INTRODUCTION

Traditionally, lenders met personally with clients to close a loan, conducting in-person closings where the borrower executed the critical loan documents before bank personnel and a notary public. Such closings provided the bank visual assurance that the borrowers had the opportunity to review the transactional documents and that the principals properly executed the loan documents. Modern consumers now expect lenders to offer the convenience and speed afforded by digital technology—enabling them to execute loan documents from the convenience of their house without burdening them with the inconvenience of attending an in-person closing. However, the convenience afforded by digital lending creates a degree of separation and anonymity, thereby increasing the risk of fraud.[2]

There is, however, a distinct difference between email/scanners and secured digital technology. Email may be a substitute for overnight

[1] The authors would like to thank Matthew Loffredo for his assistance researching and drafting this article.

[2] Andy Crisenbery, *Technology that Makes Sense for the Digital Mortgage Closing Community* (Feb. 20, 2018), https://www.alta.org/news/news.cfm?20180220-Technology-that-Makes-Sense-for-the-Digital-Mortgage-Closing-Community; AM. BANKERS ASS'N, THE STATE OF DIGITAL LENDING: RESULTS OF AN AMERICAN BANKS ASSOCIATION RESEARCH STUDY 10-11 (2018), https://www.aba.com/Products/Endorsed/Documents/ABADigitalLending-Report.pdf.

Scott L. Schmookler is a partner and Katherine Musbach is senior counsel with Gordon Rees Scully Mansukhani, LLP in Chicago, Illinois.

courier services, but in an age of data breaches, emails provide limited security; scanned copies may be a temporary substitute for the later-delivered inked originals, but in an age of digital manipulation, a scanned copy provides limited assurance of authenticity. There is, however, sophisticated technology which allows parties to attach and associate digitized signatures to documents delivered and retained digitally. The nature of each alternative and security strengths of each approach dictates the risk to financial institutions. While a fraudster can easily manipulate scanned copies of documents and blur forgeries thereon, digitized signatures provide additional authentication protections better enabling a financial institution to verify the signature and track alterations to loan documents.

Intending to facilitate electric commerce, Congress and state legislatures enacted legislation to encourage financial institutions to implement digital technology and digitize their business operations.[3] Neither the UETA nor E-SIGN created new legal rules for electronic commerce, but rather equated digital transactions with paper transactions—ensuring that electronic contracts would generally be treated as the equivalent of a paper record, and that an electronic signature would generally be given the same legal effect as a signed-in-ink signature. These laws do not, however, address the increasing risk of fraud created by digital transactions. The inconvenience of an in-person loan closing provided the bank the opportunity to verify and authenticate its client. The potential anonymity of digital transactions increases the risk of impersonation and forgery—a fact borne out by an increase in fraud-related losses.[4]

This article explores the current state of digital transactions, focusing on federal and state law governing digital transactions and their

[3] *E.g.*, Unif. Elec. Transactions Act, 7A U.L.A. 225 (1999) [hereinafter "UETA"]; 15 U.S.C. §§ 7001-7031 (2012) [hereinafter referred to as E-SIGN].

[4] For example, fraud involving losses from new loans grew 112% between 2014 and 2015, and increased another 43% in 2016. AL PASCUAL, SEAN SPOSITO & JAMES WILSON, DIGITAL LENDING FRAUD 11 (Nov. 2017), https://www.miteksystems.com/resources/2017-digital-lending-fraud-report?confirmed=1; *see also* Rogger Nettie, *E-Signatures: A New Avenue for Forgery?* (September 13, 2010), http://news.cuna.org/articles/36633-e-signatures-a-new-avenue-for-forgery.

potential impact on financial institution bonds.[5] As currently structured, existing laws have limited impact on financial institution bonds because laws regulating digital transactions and digital signatures do not apply to private transactions (absent consent of both parties) and both E-SIGN and UETA impose heightened restrictions on transactions involving negotiable instruments. However, the proliferation of digital transactions will likely increase market pressure to modernize financial institution bonds. Thus, understanding the advantages and risks posed by digital transactions and the regulation of such transactions provides insight into the risks faced by financial institutions and an opportunity to evaluate the insurability of such transactions.

II.
COVERAGE UNDER INSURING AGREEMENT (E) OF A STANDARD FORM 24 FINANCIAL INSTITUTION BOND

Therefore, before exploring the use and regulation of digital transactions, it is important to first understand the basic elements of coverage under Insuring Agreement (E). Financial institution bonds do not provide blanket coverage for all forgery-related losses. In contrast to Insuring Agreement (A) (which covers certain losses due to employee dishonesty, regardless of how the employee perpetrates the fraud),[6] Insuring Agreement (E) covers specific risks, subject to specific elements of coverage.[7] Accordingly, the methodology used by the wrongdoer to perpetrate the fraud and the insured's handling of the underlying transaction will, in many instances, dictate the existence of coverage.

Insuring Agreement (E) codifies the basic premise that financial institution bonds are not "credit insurance."[8] The bond does not "protect

[5] This article will analyze coverage for check fraud losses primarily under the 1986 edition of the Standard Form No. 24 Financial Institution Bond because despite subsequent versions, this edition remains the prevalent version. Financial Institution Bond, Standard Form No. 24 (revised to April 1986), *reprinted in* STANDARD FORMS OF THE SURETY ASS'N OF AMERICA [hereinafter 1986 Financial Institution Bond].

[6] 1986 Financial Institution Bond.

[7] *Id.* at Insuring Agreement (E).

[8] Liberty Nat'l Bank v. Aetna, 568 F. Supp. 860, 866 (D.N.J. 1983).

[an insured] when it simply makes a bad business deal."[9] "The failure to follow sound business practices and verify the authenticity is a business risk taken by [the insured] and not an insured risk covered by the Bond."[10] Requiring an insured must follow reasonable banking standards, the bond covers transactions involving specifically enumerated documents bearing a qualifying impairment, but only if the insured applies traditional banking practices and obtains the original loan documents before extending credit.[11] To that end, Insuring Clause (E) limits coverage to:

> (E) Loss resulting directly from the Insured having, in good faith, for its own account or for the account of others,
>
> (1) acquired, sold or delivered or given value, extended credit or assumed liability, on the faith of, any original
>
> (a) Certificated Security,
> (b) Document of Title,
> (c) deed, mortgage or other instrument conveying title to, or creating or discharging a lien upon, real property,
> (d) Certificate of Origin or Title,
> (e) Evidence of Debt,
> (f) corporate, partnership or personal Guarantee,
> (g) Security Agreement,
> (h) Instruction to a Federal Reserve Bank of the United States, or
> (i) Statement of Uncertificated Security of any Federal Reserve Bank of the United States

[9] Republic Nat'l Bank v. Fid. & Guar. Co., 894 F.2d 1255, 1263 (11th Cir. 1990).

[10] Nat'l City Bank v. St. Paul, 447 N.W.2d 171, 177 (Minn. 1989); 9A J. APPLEMAN & J. APPLEMAN, INSURANCE LAW AND PRACTICE § 5701, at 380 (1981) (a bond "does not insure good management nor against the risk of loss inherent in the banking operations" "punctuation").

[11] 1986 Financial Institution Bond.

which

(i) bears a signature of any maker, drawer, issuer, endorser, assignor, lessee, transfer agent, registrar, acceptor, surety, guarantor, or of any person signing in any other capacity which is a Forgery, or

(ii) is altered, or

(iii) is lost or stolen;

(2) guaranteed in writing or witnessed any signature upon any transfer, assignment, bill of sale, power of attorney, Guarantee, endorsement or any items listed in (a) through (h) above;

(3) acquired, sold or delivered, or given value, extended credit or assumed liability, on the faith of any item listed in (a) through (d) above which is a Counterfeit.

Actual physical possession of the items listed in (a) through (i) above by the Insured, its correspondent bank or other authorized representative, is a condition precedent to the Insured's having relied on the faith of such items.

A reproduction of a handwritten signature is treated the same as the handwritten signature.[12]

[12] 1986 Financial Institution Bond, Insuring Agreement (E).

These elements of coverage implicate two principal[13] issues: (1) did the insured extend credit in reliance on an enumerated document bearing a covered impairment, for example, a forgery or alteration? and (2) did the insured obtain the "original" prior to extending credit? Given these agreed elements of coverage, the form of the transaction and handling of the loan closing directly bear on the existence of coverage and the allocation of risk between the insurer and insured.

A. Contractual Definitions of Forgery and Alteration

The growing use of technology-enabled processes exposes lenders to a wide variety of crime. Fraud spans theft of data (leading to theft of financial assets), to theft of confidential data (that can be used to assemble an attack on financial assets), to traditional check fraud, to forgeries and alterations. Insuring Agreement (E) focuses on two traditional fraud-related risks: forgery and alteration. It is not, therefore, enough for a financial institution to allege fraud. Unless the claim involves a covered impairment, coverage does not apply. Therefore, before delving into digital transactions and digital signatures, it is important to first understand the type of fraud covered by Insuring Agreements (E).

1. Definition of Forgery

Prior to 1980, financial institution bond forms did not define "forgery." Courts, therefore, applied varied interpretations based upon local criminal and civil law. While the majority of courts interpreted the word narrowly and limited coverage to instances when a person signed the name of another without authority,[14] some courts applied a broad

[13] This article will not address the types of documents covered under Insuring Agreements (D) and (E). For a discussion of that issue, *see* Michael Keeley et al, *Insuring Clause (E)—Revisited*, 17 FID. L.J. 203 (2011); Peter C. Haley, *Coverage under Insuring Agreement (E) of the Financial Institution Bond, in* Financial Institution Bonds 385 (Duncan Clore, 3d ed. 2008); Scott L. Schmookler, *Insuring Agreement (D), in* Financial Institution Bonds 313 (Duncan Clore, 3d ed. 2008).

[14] *E.g.*, Reliance Ins. Co. v. First Liberty Bank, 927 F. Supp. 448 (M.D. Ga. 1996); Ralston Bank v. Kan. Bankers Sur. Co., 794 F. Supp. 896 (D. Neb 1992); French Am. Banking Corp. v. Flota Mercant Grancolombiana S.A., 752

definition, holding that "forgery" included any signature applied without authority, even if one signed his own name.[15]

Filor, Bullard & Smyth illustrates the breadth of the common law interpretation of forgery.[16] The Second Circuit held that the signature of a dishonest bank president constituted a forgery under a brokers blanket bond, even though the president signed his own name:

> One construction of the term "forgery" in favor of the insured also strikes us as being in accord with the intent of the parties. Absent a specific exclusion, [the insured] reasonably could have assumed that the blanket brokers bond covered a known risk as a loss sustained as the result of an unauthorized signature.[17]

To prevent such a broad interpretation, the Surety Association of America revised the standard form financial institution bond in 1980 to incorporate an express definition of forgery. The definition clarified that the signing of one's own name does not constitute a forgery in two respects. First, the bond defined forgery as the "signing of the name of another person or organization with the intent to deceive."[18] Second, the definition expressly provided that forgery does not mean "a signature which consists in whole or in part of one's own name signed with or without authority, in any capacity, for any purpose."[19]

The court recognized the impact of this revision in *French American Banking Corp. v. Flota Mercant Grancolumbiana S.A.*[20] Relying upon the decision in *Filor*, the insured argued that an unauthorized signature constitutes a forgery within the meaning of a financial institution bond. The court distinguished *Filor* on the basis that

---

F. Supp. 83 (S.D.N.Y. 1990); Marsh v. Langford, 554 F. Supp. 800 (E.D. La. 1982), *aff'd*, 784 F.2d 184 (5th Cir. 1982).

[15] Filor, Bullard & Smyth v. Ins. Co. of N. Am., 605 F.2d 598, 604-05 (2d Cir. 1978).

[16] *Id.* at 598.

[17] *Id.* at 601.

[18] 1986 Financial Institution Bond, § 1(i).

[19] *Id.*

[20] 752 F. Supp. 83, 90 (S.D. N.Y. 1990).

the bond was thereafter revised to incorporate an express definition of forgery and held that, under the bond's definition of forgery, the signing of one's own name, even without authority, did not constitute a forgery:

> [The insured's] reliance on [*Filor*] for the proposition that the definition of forgery under New York law is ambiguous, and therefore the term "forgery" as used in the Bond must be construed against [the insurer], is misplaced. That case held that "forgery" in a broker's blanket bond was ambiguous. The Second Circuit then construed that term against the insurer and found an unauthorized signature to constitute a "forged" signature. The Second Circuit hinged its finding of ambiguity on a revision to the New York penal law in 1967 that expanded the definition of forgery to include "writings unauthentic because not authorized." [citation omitted] However, [*Filor*] involved bonds that did not define forgery. Here, the Bond expressly provides that forgery "does not include signing one's own name with or without authority, in any capacity, for any purpose."[21]

The mere fact that the documents were used to perpetrate a fraud does not itself prove a forgery.[22] The Eastern District of New York recognized this principle in *Suffolk Federal Credit Union v. CUMIS Insurance Society Inc*., holding that counterfeit assignments neither bore a forgery nor were altered since it was "undisputed" that the employees of the loan servicer signed their own names on the assignments.[23]

In some instances, riders expand the definition of "forgery." Even then, courts look to the bond to avoid an "overly expansive"

---

[21] *Id.*

[22] Milwaukee Area Tech. Coll. v. Frontier Adjusters, 2008 WI App 76 *15, 752 N.W.2d 396, 403 (Wis. Ct. App. 2008) (finding no coverage under Insuring Agreement (D) because "that the genuine instrument was made or issued to further a criminal or fraudulent scheme does not change things" "punctuation").

[23] 910 F. Supp. 2d 446, 460 (E.D.N.Y. 2012).

definition.[24] In *Citibank Texas v. Progressive Casualty Insurance Co*., the Fifth Circuit Court of Appeals ruled that a rider which enlarged "forgery" to include "unauthorized endorsements" was "not intended to insure against endorsements by endorsers . . . who are authorized but simply exceed the scope of their endorsement authority."[25] The rider "expressly" limited such "unauthorized endorsements" to non-forgery endorsements by bank employees whose names were not on file for a given account.[26] The court held that even though the UCC may consider the employee's endorsement unauthorized, the court was "bound by the precise language of the Bond" to find that there was no forgery pursuant to either the bond's forgery definition or the expanding rider.[27]

Because of the increasing use of email communications and digital transactions, an insured may argue that a typed name constitutes a forgery. Putting aside whether a typed name qualifies for protection under existing federal and state laws, a typed name does not qualify as a forgery under the plain meaning interpretation of the bond. The bond does not define forgery as typing of a name. It requires the "signing of the name of another natural person or organization, with the intent to deceive, but does not mean a signature that includes, in whole or in part, one's own name . . . ."[28] The words "signing" and "signature" require a distinctive or stylized presentation of a name[29] and thus, the mere typing

[24] Citibank Tex., N.A. v. Progressive Cas. Ins. Co., 522 F.3d 591, 595-96 (5th Cir. 2008).

[25] *Id*. at 596.

[26] *Id*.

[27] *Id*. at 597.

[28] 1986 Financial Institution Bond, § 1(i). While the policy's definition of **Forgery** references "mechanically" reproduced signatures, this phrase does not encompass the typing of a name in an email. This phrase encompasses "'a signature that has been prepared and reproduced by mechanical or photographic means,' in other words, a signature that was generated by some mechanical process, rather than by a handwriting." Bancinsure, Inc. v. Marshall Bank, N.A., 400 F. Supp. 2d 1140, 1143-1144 (D. Minn. 2005).

[29] MERRIAM-WEBSTER, https://www.merriam-webster.com/ dictionary/ signature (last visited June 5, 2018) ("a person's name written in that person's handwriting"); OXFORD DICTIONARIES, https://en.oxford dictionaries.com/ definition/signature (last visited June 5, 2018) (signature is a "name written in a distinctive way as a form of identification in authorizing a che[ck] or document or concluding a letter").

of a name does not qualify as the signing of or a signature on a loan document.[30]

Parma Tile demonstrates why the electronic addition of a name does not constitute a signature. In that case, the plaintiff argued that a document sent via facsimile bore a "signature" because the defendant programmed a fax machine to imprint its name on every page. Even though the sender intentionally imprinted its name on the document, the New York Court of Appeals rejected the notion that the typed name constituted a "signature."[31]

Elmer Fox reached the same conclusion while interpreting forgery coverage. The bank argued that a check was forged because it was endorsed with a stamp containing the payee's name. The court disagreed, holding that a stamped name was not a signature: "[The] rubber stamp endorsement consists of the words "For deposit only" with the name and address of the company. This is not a signature."[32]

2. Definition of Alteration

Although the 1986 Financial Institution Bond includes an express definition of forgery, it does not define "alteration." Absent a specific definition, most courts have applied the UCC's definition. However, because the UCC's definition of alteration was revised in 1990, the scope of coverage afforded by the bond depends on whether the state law governing the claim has adopted the "old code" or the "new code."[33]

Prior to 1990, the UCC defined alteration as "any alteration of an instrument is material which changes the contract of any party thereto in a material respect, including any such change in (a) the number or

---

[30] *See*, *e.g.*, Elmer Fox & Co. v. Commercial Union Ins. Co., 274 F. Supp. 235, 239-240 (D. Colo. 1967); Parma Tile v. Estate of Fred, 663 N.E.2d 633, 635 (N.Y. 1996).

[31] *Parma Tile*, 663 N.E.2d at 634-35.

[32] *Elmer Fox & Co.*, 274 F. Supp. at 240.

[33] The UCC was substantially revised in 1990. The code in effect prior to 1992 is commonly referred to as the "old code," while the revised code is commonly referred to as the "new code."

relations of the parties; or (b) an incomplete instrument, by completing it otherwise than as authorized; or (c) the writing as signed, by adding to it or removing any part of it."[34] Although courts construing bond claims involving alterations generally applied the UCC's definition of "alteration," they disagreed over whether the UCC's definition should be applied according to its plain terms.[35] A minority applied a broader interpretation (because the UCC's definition required proof of materiality, while Insuring Agreement (D) did not).[36]

For example, in *St. Paul Fire & Marine Insurance Company v. State Bank of Salem*,[37] a depository bank sought indemnity for losses resulting from its payment of a check on which the amount in words had been erroneously imprinted by a check writing machine for $100,000 more than intended. After the check was issued (but before it was cashed), the amount in figures was crudely altered by the payee to correspond to the erroneous amount in words. The insurer argued that the alleged alteration of the amount in figures alone was not covered under the bond because it did not constitute a "material alteration," as defined by the UCC. The insured argued that it should not have to prove materiality because Insuring Agreement (D) did not so require. The Indiana Appellate Court disagreed:

> The Bank would have us adopt a different interpretation of alteration but we think that the meaning of the term under the U.C.C. is appropriate here. It is difficult to see how one could suffer a loss due to an alteration that is not material, and the Bank shows us none.[38]

The Missouri appellate court reached the opposite conclusion in *Stix*. In that case, a stock brokerage firm brought suit against its insurer to recover losses sustained as a result of its acceptance of altered stock

---

[34] UCC § 3-407 (AM. LAW INST. & UNIF. LAW COMM'N 1962) [hereinafter UCC].

[35] St. Paul Fire & Marine Ins. Co. v. State Bank of Salem, 412 N.E.2d 103 (Ind. Ct. App. 1980).

[36] Stix Friedman & Co. v. Fid. & Deposit Co. of Md., 563 S.W.2d 517 (Mo. Ct. App. 1978).

[37] *State Bank of Salem*, 412 N.E. 2d at 103.

[38] *Id.* at 113.

certificates. Applying the UCC's definition of alteration, the trial court instructed the jury that the insured's claim was not covered unless the alteration "materially affect[ed] the rights and obligations of the parties." The Missouri court, however, rejected this instruction:

> This definition would be proper if plaintiff were seeking to be discharged from a contract because of a material alteration in the terms of an agreement made on a written contract by the other party but it is not proper where the only issue is whether these certificates have been "raised or otherwise altered" within the meaning of this insurance policy. The policy does not require that the alteration be material.[39]

The 1990 revisions to the definition of alteration resolved this split, eliminating the materiality requirement. Alteration is now defined as "(i) an unauthorized change in an instrument that purports to modify in any respect the obligation of a party, or (ii) an unauthorized addition of words or numbers or other change to an incomplete instrument relating to the obligation of a party."[40] In effect, an insured must prove the instrument bore an unauthorized change on the instrument that modified the obligations of the drawer.

In *Bidwell & Co. v. National Union Fire Insurance Co.*,[41] two checks were intercepted and deposited into the thief's bank account. The payee line on one of the checks was changed to reflect the payee was "Bidwell & Company for: Michael Lang," prior to deposit, while the other check was deposited as drawn. When the drawer discovered the fraud, it sought indemnity under a commercial crime policy, alleging that the checks were covered under its depositor's forgery coverage because the checks had been altered. The court agreed that changing the payee on the first check constituted an alteration because it modified the obligation

[39] *Stix Friedman & Co.*, 563 S.W.2d at 521.

[40] UCC § 3-407(a).

[41] Bidwell & Co. v. Nat'l Union Fire Ins. Co., No. CV-00-89-HU, 2001 WL 204843, at *7-8 (D. Or. Jan. 18, 2001).

of the drawer, but it rejected the insured's argument that depositing of the second check into the thief's account constituted an alteration.[42]

An insured must still prove a modification of the instrument. The mere allegation that the document was used to perpetrate a fraud or contained a misrepresentation is insufficient to establish an alteration. For example, in *Northside Bank v. American Casualty Co.*,[43] a company opened an account under a merchant services agreement with a bank. Pursuant to this agreement, the company began accepting merchandise orders and taking payment by debit and credit cards. The transactions were transmitted to the bank electronically and upon receipt, the bank would transfer money to the company's account. After the company failed to deliver the merchandise to its customers, the bank sought recovery under its financial institution bond, arguing that the electronic instructions were altered because they contained a misrepresentation. The court rejected this argument, holding that the electronic instructions could not have been altered because they were never modified. "The simple truth is that the words 'modified' and 'altered' mean exactly what they say."[44]

In *Utica Mutual Insurance Co. v. Precedent Cos.*,[45] the insured issued a check payable to a title company to fund a residential loan. Although the loan did not close and was not funded, the title company deposited the check into its account. Upon discovery, the insured sought indemnity for its loss, alleging that the title company altered the check by depositing it into its account. Applying the revised definition of alteration, the Indiana Appellate Court rejected this argument, holding that merely depositing a check contrary to or in breach of a contractual agreement did not constitute an alteration:

> Again, [the insured] does not allege, and the undisputed facts do not show, that [the insurer] made any unauthorized change in or on the instrument. Nor did [the insurer] add words or numbers to the instrument,

[42] *Id.*

[43] Northside Bank v. Am. Cas. Co. of Reading, No. GD 97-19482, 2001 WL 34090139 (Pa. C.P. Jan. 10, 2001).

[44] *Id.* at *2.

[45] 782 N.E.2d 470 (Ind. Ct. App. 2003).

> and the instrument was complete when [the insurer] received it.[46]

B. Actual Physical Possession of the Original Instrument

An insured's loss, even if due to a forged or altered document, is not covered unless the insured physically possessed the "original" document when it extended credit.[47] Financial institution bonds require an insured to obtain original documents (in lieu of copies) because a financial institution cannot viably evaluate the existence of a forgery without inspecting the original instrument. The absence of original documents limits analysis of a questioned document to the limited features surviving the copying process.

By its nature, handwriting is a complex motor skill combining sensory, neurological, and physiological impulses. Factors such as visual perception and acuity, comprehension of form, central nervous system pathways, and the anatomy and physiology of the bones and muscles of the hand and arm combine to produce an individualized result.[48] Because mastering the act of handwriting requires practice and repetition, our writing becomes a pattern of habitual formations repeated from one writing to the next.[49]

Comparing and evaluating these individual features/habits enable document examiners to identify or exclude a known writer as the source of a questioned writing. Examiners complete this analysis by evaluating various factors, including the size and slope of the writing, pen pressure, pen lifts, the spacing between words and letters, the position of the writing on the baseline (the position of the character in relation to the ruled or imaginary line), height relationships, beginning and ending strokes, and line quality.[50]

---

[46] *Id.* at 477.

[47] Financial Institution Bond, Insuring Agreement (E).

[48] ROY A. HUBER & A.M. HEADRICK, HANDWRITING IDENTIFICATION: FACTS AND FUNDAMENTALS, 10-14 (1999).

[49] ORDWAY HILTON, SCIENTIFIC EXAMINATION OF QUESTIONED DOCUMENTS, 10, 17, 153-57, 174 (2d ed. 1992).

[50] *Id.*

"The *principle of individuality*, also known as the *principle of uniqueness*, forms the basis for any handwriting analysis."[51] Each person writes differently, even within repetitions of writings. "This is known as natural variation, or intra-writer variation."[52] The copying process impacts critical features directly bearing on an examiner's ability to detect and report a forgery because while originals disclose all of the physical and optical features of the printing processes and handwriting features, copies remove features present in the original images.

The difference results in a loss of intricate pen direction, tapered strokes, and hesitations—all of which leave an examiner unable to render a conclusive opinion on whether a questioned and known writing were not prepared by the same writer because of sufficient disagreement in individual characteristics.[53] Understanding how the failure to maintain an original impacts an examiner's ability to evaluate the existence of a forgery demonstrates the rationale for conditioning forgery coverage on the possession of such documents.

- ***Pen Detail*** represents intricate writing movements essential for reaching an accurate conclusion about the existence of a forgery.[54] The inability to inspect and maintain the original document impacts an examiner's ability to analyze those details and thus, his ability to detect forgery.

[51] Diana Harrison et al., *Handwriting Examination: Meeting the Challenges of Science and the Law*, 11 Forensic Science Communications (2009).

[52] *Id.*

[53] Each analysis begins with an independent examination of the questioned and then the known writing using proper lighting and magnification to determine if the writing is original writing (e.g., ink on paper) and whether it exhibits the characteristics of freely and naturally prepared writing. ASTM INTERNATIONAL, E2290-07A STANDARD GUIDE FOR EXAMINATION OF HANDWRITTEN ITEMS (2007) *available at* http://www.astm.org/Standards/E2290.htm.

[54] Linda Mitchell, *Photocopies for Evidence—Beware*, FORENSIC DOCUMENT EXAMINER, (Jan. 12, 2012), https://www.forensicdocexaminer.com/photocopies-for-evidence-beware/.

- ***Tapered Strikes*** enable an examiner to analyze the blunt ending and beginning strokes for characteristics of "signatures" produced through simulation or tracing. The copying process can eliminate these tapered strokes and make them appear as blunt in an otherwise naturally executed signature.[55] "This can be likened to identifying a person behind a cloudy window; the basics are there, but details are missing."[56]

- ***Line Quality*** represents the thickness, strength, and flow of the letters.[57] Under magnification, examination of the original line quality may reveal indicia of forgery (*e.g.*, granulated strokes, resting spots, tremulousness, jerkiness)."[58] A photocopy of a genuine signature may show "lumpiness" or lack of smooth, clear-cut strokes, resulting in poor record of the strokes—thereby preventing an unqualified opinion about the existence of a forgery.

- ***Hesitations*** represent a pause in the writing line. Confidence in a signature, due to repeated use and familiarity, leads to a fluid line. Hesitations are common artifacts of "forged" signatures and may reveal careful retouching sometimes seen in "forged" signatures as a result of the thief's perception that the simulation or tracing needs some mending to pass it off as genuine.[59]

---

[55] *Id.*

[56] *Id.*

[57] Katherine Frazier, *12 Handwriting Characteristics*, FORENSICS BLOG (Nov. 18, 2011, 8:50 AM), http://kfrazierforensics.blogspot.com/2011/11/12-handwriting-characteristics.html.

[58] MARC SEIFER, *THE DEFINITIVE BOOK OF HANDWRITING ANALYSIS (2009); MICHAEL P. CALIGIURI & LINTON A. MOHAMMED, THE NEUROSCIENCE OF HANDWRITING (2012).*

[59] The result of this is a signature where the forger hesitates mid-way to consider the next letter or the correct flow. Handwriting forensics experts can tell when a pen has stopped in the middle of the signature. Teresa DeBerry, *Key Indicators of Forgery in Handwriting Forensics*, HANDWRITING FORENSICS BLOG (Mar. 3, 2017), http://teresadeberry.com/key-indicators-forgery-handwriting-forensics/.

> An examiner cannot, however, generally detect hesitation and retouching in a copy.

Given the impact of failing to maintain original documents, courts strictly enforce the plain terms of Insuring Clause (E), holding that an insured's failure to obtain the original precludes coverage.[60] The Ninth Circuit upheld the original requirement in *Bank of Bozeman*. In that case, the insured purchased an interest in a loan allegedly based upon forged stock certificates. Because the insured never obtained the original stock certificates, the Ninth Circuit held that the insured could not recover under Insuring Agreement (E): "[a] condition precedent to coverage under BancInsure's Financial Institution Bond (FIB) is 'actual physical possession of [original security documents] by the Insured . . . or [its] authorized representative.'"[61]

Hamilton Bank reached the same conclusion. In that case, the plaintiff made sixteen loans to an importing company in reliance upon photocopies of certain bills of lading. When the borrower defaulted, the insured sought indemnity under its financial institution bond. The insurer denied coverage because, although the insured sustained a loss as a result of its reliance on forged documents, it did not possess the original bills of lading at the time of the loan. Affirming summary judgment, the Pennsylvania Appellate Court agreed:

> [T]he clear meaning of the blanket bond mandates that [the insured] must physically possess the original bills of lading at the time of extending credit before it may recover its losses. . . . [The insured] contends that . . . [its] possession of *photocopies* of the original counterparts of the bills of lading is sufficient. . . . [T]here can be no doubt that, considering the situation before us, mere *photocopies* of the original counterparts

[60] Bank of Bozeman v. BancInsure, No. 09-36088, 404 F. App'x 117 (9th Cir. 2010); BancInsure v. Marshall Bank, 453 F.3d 1073, 1076 (8th Cir. 2006); Reliance v. Capital Bankshares, 912 F.2d 756, 758 (5th Cir. 1990); First Nat'l Bank v. Hartford Accident & Indem. Co., 295 N.W.2d 425, 429 (Iowa 1980); Nat'l City Bank v. St. Paul, 447 N.W.2d 171, 177 (Minn. 1989); Hamilton v. INA, 557 A.2d 747, 750 (Pa. Super. Ct. 1988).

[61] 404 F. App'x at 118.

> of the bills of lading do not qualify as "original" documents. We find it ludicrous that [the insured], which certainly would not honor a photocopy of a check of nominal value, has the audacity to contend that it is reasonable to lend $1.4 million based upon mere photocopies of duplicate bills of lading.
>
> . . . .
>
> In sum, we find that the bankers blanket bond is clear and free from ambiguity. In order to recover under the provisions of the bond, we find that [the insured] would have needed to extend the credit in reliance on original bills of lading (not mere photocopies thereof) which should have been in [its] physical possession prior to release of funds. Since no genuine issues of material fact remain and, based upon our interpretation of the bankers blanket bond, [the insurer] is entitled to judgment as a matter of law. . . .[62]

The Eighth Circuit enforced the original requirement despite possession of an electronic copy in *Marshall Bank*. In that case, the insured submitted a financial institution bond claim, alleging that a thief fraudulently induced it to approve a loan based upon forged loan documents. The insured did not, however, obtain the original loan documents before extending the loan and disbursing the loan proceeds. Instead, it accepted a facsimile copy of the loan documents. The failure to procure the original, the court held, precluded coverage:

> By its own terms, the clause at issue speaks to what type of signature is acceptable. It does not, however, except the bank from maintaining actual physical possession of the original guarantee . . . .[63]

The insured argued that requiring original documents rendered coverage meaningless, but court rejected that argument:

---

[62] 557 A.2d at 750-51.
[63] 453 F.3d at 1076-77.

> Again, we cannot agree that the coverage against forgery that Marshall Bank purchased was meaningless. The protection afforded by the policy is against forgery, but not forgery committed by use of faxed documents, accepted by the bank without perusal of the originals. Several factual scenarios, all involving forgery, would have clearly resulted in coverage under the policy. Most notably, Marshall Bank could have simply waited for original documents to arrive before disbursing funds. The fact that an insured's circumstance is outside a policy's realm of coverage does not, without more, render the policy illusory. Marshall Bank paid for protection from forgery and, in most instances, the policy provided that coverage. This is not one of those instances, however, and we will not read such coverage into the policy.[64]

It so held because the bond does not "permit[] copied documents to serve as proxies for originals."[65]

III.
REGULATION OF ELECTRONIC TRANSACTIONS AND SIGNATURES

Prior to 1999, various states enacted sporadic laws to address digital transactions. In 1999, the National Conference of Commissioners on Uniform State Laws promulgated UETA as a means of providing uniformity to emerging digital commerce.[66] One year later, President Clinton signed E-SIGN—a law designed to resolve points of non-uniformity among the states that had not adopted UETA and as a backstop to better regulate digital commerce.[67] This article will briefly explore E-Sign and the state regulation of digital transactions and signatures.

---

[64] *Id.*
[65] *Id.* at 1076.
[66] 7A U.L.A. 225 (1999).
[67] 15 U.S.C. §§ 7001-7031 (2012).

A. Federal Legislation

In 2000, Congress passed E-SIGN, granting federal recognition to electronic signatures used in interstate and international electronic transactions.[68] Enacted in recognition of "[t]he growth of electronic commerce" and acknowledgment that these "transactions represent[] a powerful force for economic growth,"[69] Congress sought to adopt a consistent legal foundation based upon "technology neutral" regulation.[70] E-SIGN did not advance the discussion of and use for technology, but instead sought:

> (1) to permit and encourage the continued expansion of electronic commerce through the operation of free market forces rather than proscriptive governmental mandates and regulations;
> (2) to promote public confidence in the validity, integrity, and reliability of electronic commerce and online government under Federal law;
> (3) to facilitate and promote electronic commerce by clarifying the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law;
> (4) to facilitate the ability of private parties engaged in interstate transactions to agree among themselves on the terms and conditions on which they use and accept electronic signatures and electronic records; and
> (5) to promote the development of a consistent national legal infrastructure necessary to support electronic commerce at the Federal and State levels within existing areas of jurisdiction.[71]

E-SIGN does not therefore directly bear on the appropriate integration of digital lending transaction and the authentication of digital

[68] *Id.*
[69] H. R. REP. No. 106-341, pt. 2, at 2 (1999).
[70] *Id.*
[71] *Id.* at 3.

signatures.[72] In fact, E-SIGN does not even require the use of "electronic signatures." Instead, it simply provides that electronic signatures or records may not be denied legal effect solely because they are electronic:

> Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II of this chapter), with respect to any transaction in or affecting interstate or foreign commerce—
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
> (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[73]

E-SIGN has limited effect on private transactions in that it does not alter existing laws or contractual obligations. E-SIGN does not "limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law" except a "requirement that contracts or other records be written, signed, or in nonelectronic form."[74] The latter could be misread to suggest that E-SIGN impacts the insured's obligation to maintain original documents, but absent express agreement of the parties, E-SIGN has no impact on private contracts as it does not "require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party."[75]

---

[72] Designed to be "technology neutral," E-SIGN does not contain any requirement that parties use certain technologies to authenticate the electronic signature. *See* Anda Lincoln, Comment, *Electronic Signature Laws and the Need for Uniformity in the Global Market*, 8 J. SMALL & EMERGING BUS. L. 67, 73 (2004); Adam R. Smart, Note & Comments, *E-Sign Versus State Electronic Signature Laws: The Electronic Statutory Battleground*, 5 N. C. BANKING INST. 485, 493 (2001).

[73] 15 U.S.C. § 7001(a) (2012).

[74] *Id.* § 7001(b).

[75] *Id.*

B. State Legislation

While Congress adopted E-SIGN, it did not preempt[76] all state legislation on digital transactions and digital signatures.[77] Section 102(a) of E-SIGN specifies that state law may modify, limit or supersede the electronic contracting provisions of E-SIGN under limited conditions. Under sub-part (1), state law may modify, limit or supersede the federal legislation if it "specifies the alternative procedures or requirements for the use or acceptance of electronic records or electronic signatures, provided:

> (a) any alternative procedures or requirements are consistent with Titles I and II and
>
> (b) the alternative procedures do not require, or give greater legal status or effect to use or application of a specific technology or technological specification.[78]

Thus, states are free to enact an e-signature law that contains provisions outside the scope of E-SIGN—such as provisions governing attribution of electronic signatures, the time when messages are deemed sent or received, the effect of change or error in an electronic record, and admissibility of electronic records and signatures in evidence, or the transferability of records.

---

[76] Preemption is often moot as in many instances there will be no difference between an outcome under E-SIGN and state laws. D. Benjamin Beard, *Uniform Electronic Transactions Act in* 10 HAWKLAND UNIFORM COMMERCIAL CODE SERIES § 3.3 (Thomson/West Pub., 2007); People v. McFarlan, 744 N.Y.S.2d 287, 294 (N.Y. Sup. Ct. 2002) ("Although there are clear conflicts between E Sign and [the New York statute, ESRA,] for many purposes, the same result would obtain in this case whether E-Sign or ESRA applies, and accordingly, the constitutional and preemption issues need not be reached in rendering this decision.").

[77] 15 U.S.C. § 7002(a)(2)(A)(ii) (2006).

[78] However, the legislative history regarding technological neutrality shows that Congress "intended to prevent a state from giving a leg up or imposing an additional burden on one technology or technical specification that is not applicable to all others . . . ." 146 CONG. REC. S5285 (daily ed. June 16, 2000) (statement of Sen. Abraham).

The majority of states adopted the Uniform Electronic Transactions Act. ("UETA")[79] without material revision. Some states (principally Washington and New York) adopted uniform acts or materially limited the scope and application of the UETA. Depending upon the governing law, these uniform acts and material revisions could substantially alter the enforceability of digital transactions and digital signatures.

1. Uniform Acts for Electronic Signatures

In 1999, the Uniform Law Commission created the Uniform Electronic Transactions Act..[80] The UETA recognized that while "business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies," these developments faced "legal requirements that raise real barriers to the effective use of electronic media."[81] UETA intended to "remove barriers to electronic commerce by validating and effectuating electronic records and signatures" by "establishing the equivalence of an electronic record . . . without affecting the underlying legal rules and requirements."[82]

To accomplish that purpose, the UETA provides legal recognition for electronic records and electronic signatures, provided that electronic records and signatures satisfy specific legal requirements.[83] Subject to the parties' right to privately contract, the UETA contemplates that a qualifying electronic signature or electronic contract will not be denied enforceability merely because of its electronic format.[84] The UETA does not apply unilaterally to parties to a transaction—the parties must agree to conduct transactions electronically, a test determined by the parties' conduct and other circumstances surrounding the transaction.[85]

---

[79] 7A U.L.A. 225 (1999).
[80] 7A U.L.A. 225 (1999).
[81] *Id.* at Prefatory Note.
[82] *Id.*
[83] *Id.* § 7(c), 7(d).
[84] *Id.* § 7(a), 7(b).
[85] *Id.* § 5(b).

The UETA defines an electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[86] It is not, therefore, enough to allege that a document bears an electronic signature; the electronic signature must be "associated with" the document:

> In order to qualify as an electronic signature, the system used to capture the transaction must (i) keep an associated record that details how the signature was created; or (ii) generate textual or graphic statement (which can be added to signed record) proving it was executed with electronic signature.[87]

The authenticity of an electronic signature may be established "in any manner, including a showing of the efficacy of any security procedure applied."[88] The effect of the signature "is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement . . ."[89] The "critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record."[90] Intent may be "shown in any manner including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable."[91]

The UETA applies to an "electronic record", defined as "a record created, generated, sent, communicated, received, or stored by electronic means."[92] Under the UETA, a record custodian must retain an electronic record which (1) accurately reflects the information in the record as it was generated in its final form; and (2) remains accessible for later reference.

---

[86] *Id.* § 2(8).
[87] *Id.* § 12(a).
[88] *Id.* § 9(a).
[89] *Id.* § 9(b).
[90] *Id.* § 2, Comment 7.
[91] *Id.* § 9(a).
[92] *Id.* § 2(7).

2. New York Electronic Signature and Records Act

In contrast to the majority of states, New York originally declined to adopt the UETA and instead adopted a manuscript act, the New York Electronic Signature and Records Act ("ESRA").[93] Signed into law on September 28, 1999 and effective March 27, 2000, the ESRA provided general authorization for the use of electronic signatures and records, and delegated to the State Office for Technology responsibility for issuing rules and regulations related to electronic transactions.[94]

Compliance with the ESRA was voluntary. It provided that "nothing in this article shall require any entity or person to use an electronic record or an electronic signature unless otherwise provided by law."[95] ESRA regulations contain a similar provision.[96] These provisions did not, therefore, directly impact the interpretation of private contracts and did not excuse a private party from fully complying with contractual agreements.[97] Nonetheless, the ESRA did not contemplate the treatment of any typed name constitutes a signature, or immunize an insured from maintaining original documents.

On the contrary, ESRA defined an "electronic signature" as: "an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record." While this definition afforded the parties to an electronic transaction flexibility in selecting an appropriate e-signature solution, it set parameters on what constitutes an authorized e-signature.

A range of digital objects could qualify as an e-signature. These objects can be as simple as a pre-authorized set of keyboarded characters,

---

[93] N.Y. State Technology Law, ch. 57-A § 101 et seq. (Consol. 1999).

[94] The ESRA designates the State Office for Technology the "Electronic Facilitator", the entity responsible for "develop[ing] guidelines for the improvement of business and commerce by electronic means" and to "identif[ing] preferred technology standards relating to security, confidentiality, and privacy of electronic signatures and electronic records." *Id.* § 103(2)(c).

[95] *Id.* § 109.

[96] *See* N.Y. COMP. CODES R. & REGS. tit. 9, § 540.1(d) (2000).

[97] *Id.*

as sophisticated as an encrypted hash or a process.[98] However, ESRA and its enabling regulation differentiated between the mere typing of a name and a qualifying digital signature by requiring an e-signature to be "attached to or logically associated with an electronic record" and proof that the e-signature reflected intent to carry out their obligations under the signed document.

First, ESRA required an e-signature to be "attached to or logically associated with an electronic record." Requiring the linking of the e-record to an e-signature differentiated a qualifying electronic signature from the mere typing of a name in that it requires a means of linking the signature to the document for future authentication and verification.[99] Under ESRA, the attachment or logical association between the signed record and signature had to be created at the point a record was executed, maintained during any transmission of the signed record, and retained for as long as the signed record is needed including any subsequent storage.

Second, ESRA required proof that the signer applied a qualifying signature with the intent to carry out their obligations under the signed document. Traditionally, the ceremonial act of signing with pen and ink warned of their legally binding commitment. ESRA codifies that process too, by requiring that an e-signature be accompanied by the same intent as the use of a signature affixed by hand. While ESRA did not require any specific level or method of signer identification or authentication, it required proof of intent. Thus, the selection of an appropriate approach to identify and authenticate a signer is a significant consideration in selecting an e-signature protocol.

---

[98] A process can create an e-signature when a system used to create a signed e-record associates the recorded events of accessing an application with the content to be signed, thereby creating a virtual record of the signer's actions and intent.

[99] That can be achieved by various means. For instance, a digital signature can be a discrete digital object that is part of the document in the same manner as an ink signature or it can be an object associated with the document through an embedded link. The signature object can also be maintained separately but logically associated with the record through a database, index, or other means.

A signer's intent could be captured in a number of ways. For example, a business can make it impossible for an e-signature to be applied to a document without the signer having been informed that a signature is being applied, format an electronically signed record to contain the same accepted signature elements captured in a paper record allowing a reader to readily identify the significance of the signature appearing on the bottom line, require the signer's intent to be expressed as part of the record or in a certification statement linked to the record, or require the signer to act affirmatively to indicate assent to the document being signed.

In 2011, the New York legislature amended ESRA, thereby more closely aligning ESRA with the UETA. ESRA broadly adopted UETA's definition of "electronic signature", defining as "an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."[100] However, an electronic signature is not automatically associated with an electronic record. "An electronic signature is considered to be 'attached to or logically associated with an electronic record' if the electronic signature is linked to the record during transmission and storage."[101]

ESRA also adopted a significant exception—limiting application of the act to transactions involving negotiable instruments:

> 307. Exceptions. This article shall not apply: . . . .
>
> To any negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title, unless an electronic version of such record is created, stored or transferred pursuant to this article in a manner that allows for the existence of only one unique, identifiable and unalterable version which cannot be copied except in a form that is readily identifiable as a copy.[102]

[100] N.Y. COMP. CODES R. & REGS. tit. 9, § 540.4(b) (2000).
[101] *Id.*
[102] New York Consolidated Laws, State Technology Law—STT § 307.

Thus, in the context of lending transactions, a financial institution cannot simply apply ESRA to any electronic record or electronic signature; to the extent that the transaction involves any form of negotiable instrument, the financial institution can only rely on ESRA if it can demonstrate that the electronic version was "created, stored or transferred . . . in a manner that allows for the existence of only one unique, identifiable and unalterable version which cannot be copied except in a form that is readily identifiable as a copy."[103]

3. Washington Electronic Authentication Act

In 1997, the State of Washington enacted the Electronic Authentication Act ("WEAA") "to facilitate commerce by means of reliable electronic messages." Designed to enhance economic development through the use of digital signatures in electronic commerce while "minimiz[ing] the incidence of forged digital signatures and fraud in electronic commerce," the act imposed stringent certification and operating standards.[104] The original WEAA gave legal significance only to digital signatures that followed specific security protocols, by defining "digital signatures" as

> a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the initial message has been altered since the transformation was made.[105]

The WEAA provided guidance for the Secretary of State to license "certification authorities"[106]—approved entities authorized to issue a "certificate." The WEAA then defined a "certificate" as:

---

[103] *Id.*

[104] WASH. REV. CODE § 19.34.010-.903 (1997).

[105] Id. § 19.34.020(11).

[106] *Id.* § 19.34.020(5) (defining "certification authority" to mean "a person who issues a certificate").

> a computer-based record that: (a) Identifies the certification authority issuing it; (b) Names or identifies its subscriber; (c) Contains the subscriber's public key; and (d) Is digitally signed by the certification authority issuing it.[107]

In 1999, the Washington legislature amended WEAA to allow for additional technologies beyond digital signatures.[108] The legislature added the terms "electronic" and "electronic signature"—defining "electronic" as an "electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies"[109] and defining "[e]lectronic signature" as "a signature in electronic form attached to or logically associated with an electronic record, including but not limited to a digital signature."[110]

However, the amendments did not alter the statutorily imposed security obligations. The legislature declined to replace "digital signature" with "electronic signature" and thus, the validity, enforceability and acceptance of an electronic document depended upon whether it bore a digital signature. Thus, "where a rule of law requires a signature . . . that rule is satisfied by a digital signature . . . ."[111] Similarly, a document is "valid, enforceable, and effective as if it had been written on paper, if it . . . [b]ears in its entirety a digital signature . . . ."[112] Thus, the legislature broadened the stated purpose of the act to include "electronic signatures," but it otherwise did not change

---

[107] *Id.* § 19.34.020(4) (defining "certificate" as "a computer-based record that: (a) Identifies the certification authority issuing it; (b) Names or identifies its subscriber; (c) Contains the subscriber's public key; and (d) Is digitally signed by the certification authority issuing it"); *see also id.* § 19.34.020(38) (defining "subscriber" as "a person who (a) Is the subject listed in the certificate; (b) Applies for or accepts the certificate; and (c) Holds a private key that corresponds to a public key listed in that certificate").

[108] Act of May 13, 1999, ch. 287, 1999 WASH. SESS. LAWS 1203.

[109] *Id.* § 3, 1999 WASH. SESS. LAWS 1207 (codified as amended at WASH. REV. CODE § 19.34.010(2)).

[110] *Id.* § 2(12), 1999 WASH. SESS. LAWS 1204 (codified as amended at WASH. REV. CODE § 19.34.020(12)).

[111] WASH. REV. CODE § 19.34.300(1).

[112] *Id.* § 19.34.320.

the underlying substantive commands of the act that give legal recognition to digital signatures.[113]

IV.
APPLICATION OF E-SIGNATURE REGULATIONS ON FINANCIAL INSTITUTION BOND CLAIMS

Financial institutions pursuing forgery claims often portray any typed name as a signature and a scanned copy of a document as an "original" on the theory that legislation encouraging digital transactions broadly defines the term "signature" and permits them to treat an electronic copy as though it were a paper copy. Such arguments, however, ignore the express limitations within the UETA and E-Sign—both of which exempt private transactions and exempt transactions involving negotiable instruments. Application of the plain terms of the UETA and E-Sign demonstrate that they have no impact on current financial institution bonds.

A. Statutory Exemption for Private Transactions

Given the proliferation of digital transactions and digital signatures, many financial institutions portray a typed named as a forgery and a scanned document as an original. This analysis, however, ignores the reality that law governing digital transactions and digital signatures exempt private transactions. Therefore, while financial institutions continue to adopt and embrace the use of digital transactions and digital signatures, these transactions do not alter the insured's contractual obligation under Insuring Agreement (E) to prove the existence of a forgery and possession of the original loan documents.

Pursuant to § 5, the UETA applies only if both parties agree to conduct transactions by electronic means.[114] Strictly enforcing this provision, courts agree that the UETA does not apply unless both parties had in fact agreed to conduct transactions electronically.[115] A party may

---

[113] *Id.* § 1(4), 1999 WASH. SESS. LAWS 1203; id. § 12(1), 1999 WASH. SESS. LAWS 1215.

[114] UETA § 5(b).

[115] Celtic Marine Corp. v. James C. Justice Cos., 760 F.3d 477 (5th Cir. 2014); Audi AG v. D'Amato, 381 F. Supp. 2d 644 (E.D. Mich. 2005), *aff'd on*

submit circumstantial evidence of such agreement, but they bear a heavy burden of proving a pre-loss or pre-default agreement.[116]

J.B.B. Investment Partners, Ltd. illustrates a strict enforcement of the UETA and refusal to enforce a digital transaction absent a prior agreement. The claim involved a dispute over whether a printed name at the conclusion of an email represented an agreement to the settlement terms outlined in the email. Reversing a judgment in favor of the investors who claimed fraud, the court held that a defendant's printed name at the end of his e-mail (where he had agreed to settlement terms set forth in an e-mail from the investors' counsel) was not an "electronic signature" within the meaning of the UETA since the investors did not demonstrate that the parties ever agreed to conduct transactions by electronic means:

> Nothing in the record indicates counsel or the court was aware of any of the provisions of UETA just cited, other

other grounds, 469 F.3d 534 (6th Cir. 2006); *In re* Rhee, 481 B.R. 880 (Bankr. S.D. Tex. 2012); J.B.B. Inv. Partners, Ltd. v. Fair, 182 Cal. Rptr. 3d 154 (Cal. Ct. App. 2014); B. Riley & Co., LLC v. NXTV, Inc., B219990, 2010 WL 5396006 (Cal. Ct. App. 2010); Sigg v. Coltrane, 253 P.3d 781 (Kan. App. 2010); White v. Strange, 80 So. 3d 1189 (La. Ct. App. 3d Cir. 2011); SN4, LLC v. Anchor Bank, FSB, 848 N.W.2d 559 (Minn. Ct. App. 2014); Powell v. City of Newton, 703 S.E.2d 723 (N.C. 2010).

[116] Cortez v. Ross Dress for Less, Inc., No. EDCV 13-01298 DDP, 2014 WL 1401869 (C.D. Cal. 2014); Williamson v. Bank of N.Y. Mellon, 947 F. Supp. 2d 704 (N.D. Tex. 2013) (applying Texas law); Rosas v. Macy's, Inc., No. CV11-7318 PSG, 2012 WL 3656274 (C.D. Cal. 2012); All. Laundry Sys., LLC v. Thyssenkrupp Materials, NA, 570 F. Supp. 2d 1061 (E.D. Wis. 2008); Brantley v. Wilson, No. 05-5093, 2006 WL 436121 (W.D. Ark. 2006); Int'l Casings Grp., Inc. v. Premium Standard Farms, Inc., 358 F. Supp. 2d 863 (W.D. Mo. 2005) (applying Missouri and North Carolina law); Dalos v. Novaheadinc, No. 1 CA-CV 07-0459, 2008 WL 4182996 (Ariz. Ct. App. 2008); McClare v. Rocha, 2014 ME 4, 86 A.3d 22 (Me. 2014); Clean Props., Inc. v. Riselli, No. 127631, 2014 WL 4082266 (Mass. Super. Ct. 2014); Crestwood Shops, L.L.C. v. Hilkene, 197 S.W.3d 641 (Mo. Ct. App. 2006); Kluver v. PPL Montana, LLC, 2012 MT 321, 293 P.3d 817 (Mont. 2012); Waddle v. Elrod, 367 S.W.3d 217 (Tenn. 2012); Cameron Intern. Corp. v. Guillory, 445 S.W.3d 840 (Tex. App.—Houston [1st Dist.] 2014, no pet.) (applying Delaware law); Dittman v. Cerone, No. 13-11-00196-CV, 2013 Tex. App. LEXIS 13404, 2013 WL 5970356 (Tex. App.—Corpus Christi Oct. 31, 2013, no pet.).

> than section 1633.7, or appreciated the complexity of the statutory scheme. Focusing only on section 1633.7, the court appears to have simplistically assumed, as did counsel for plaintiffs, that because [defendant]admitted at deposition that the signature was his, and the signature was indisputably electronic, the printed signature on the July 4 offer was therefore an "electronic signature" within the meaning of UETA.[117]

The court rejected the notion that the mere existence of a typed salutation established the existence of an e-signature subject to protection under the UETA:

> The trial court's analysis was incomplete. Attributing the name on an e-mail to a particular person and determining that the printed name is "[t]he act of [this] person" is a necessary prerequisite but is insufficient, by itself, to establish that it is an "electronic signature." (§ 1633.9, subd. (a).) As counsel and the court seemed unaware, UETA defines the term "electronic signature." Subdivision (h) of section 1633.2 states that "'[e]lectronic signature' means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record." . . . We have independently reviewed the record and conclude, as a matter of law, that it does not show that [defendant]printed his name at the end of his e-mail with any intent to formalize an electronic transaction.[118]

Sigg agreed that transmitting a document via email does not constitute a valid, enforceable digital transaction. In that case, an individual sought to enforce a contract against a husband and wife, even though none of the written or electronic documents contained the couple's signatures. The court rejected a claim that the couple's electronic drafting and e-mailing of a document constituted an agreement to conduct an electronic transaction as contemplated by the UETA:

---

[117] 182 Cal. Rptr. 3d at 164.

[118] *Id.* at 165.

> [T]here is no evidence that this transaction meets the requirements of K.S.A. 16-1605(b): "This act applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties conduct." There is absolutely nothing in the record that indicates that Sigg and the Coltranes agreed to conduct their transactions by electronic means.[119]

The mere fact that the parties agree to conduct a single transaction electronically does not provide blanket authorization to conduct all transactions electronically. For example, *SN4, LLC* involved a series of online negotiations for the purchase of property from a bank. The court affirmed a judgment for the bank on a breach of contract action because there was no subscription to an agreement as required by the statute of frauds. In so holding, the court rejecting a claim that UETA applied. The court noted the buyers' argument that ongoing e-mails illustrated a pattern of consistent, electronic communications, and provided sufficient grounds to conclude that the bank consented to transact with them electronically. The court disagreed, holding that each "transaction" had to be examined individually to determine whether the parties had agreed to conduct that specific transaction by electronic means:

> But the buyers' application of the UETA is overly broad. The UETA provides that "[i]f a party agrees to conduct a transaction by electronic means, [the UETA] does not prohibit the party from refusing to conduct other transactions by electronic means." *Id.* (c). Each "transaction"—or an action or set of actions—must be examined individually to determine whether the parties have agreed to conduct that specific transaction by electronic means. *See id.* Accordingly, while contracting parties may agree to negotiate and form a contract by electronic means, doing so does not mean that they have also agreed to electronically subscribe to whatever

[119] 253 P.3d at 785.

> agreement may result from their electronic negotiations.[120]

Therefore, even though the parties negotiated the agreement via e-mail, the court held that the agreement itself was unenforceable absent an express agreement between the buyers and the bank to electronically subscribe to the purported agreement.[121]

Resolution of such disputes generally vary based upon the circumstances underlying the transaction. For example, *Dalos* involved a dispute over whether an employer could recover on a claim for unpaid wages despite the running of a one-year limitations period. Since the employer acknowledged the debt by e-mail, the court reasoned that employer satisfied the statutory requirement of an acknowledgement. While the parties did not execute a formal agreement to conduct transactions electronically, the court noted that the UETA was intended to facilitate electronic transactions and while the UETA requires an agreement to conduct an electronic transaction, the consent to electronic communications required lesser proof:

> A person may be deemed to have consented to electronic communications by on-going participation in such communications . . . or by primary use of that medium. . . . In this case it particularly would be anomalous to suggest that Sweeney and Dalos, employees of a software company, did not consent to using e-mail.[122]

Accordingly, the ongoing participation in electronic communications reflected an agreement to abide by such form of communication.[123]

Brantley involved a real estate transaction contract completed via telephone and e-mail. The sellers alleged that emails reflected negotiations, but the court rejected that argument and found a question of fact as to the enforceability of the contract under the statute of frauds.

---

[120] 848 N.W.2d at 566-67.
[121] *Id.*
[122] *Dalos*, 2008 WL 4182996 at *9-10.
[123] *Id.*

The court held that the participation in discussions over email raised a genuine issue of material fact as to whether the sellers intended to conduct a land sale transaction involving the property by electronic means:

> The Court believes reasonable jurors could find this group of e-mails "so connected with each other that they may be fairly said to constitute one paper relating to the contract." They might also deduce therefrom that Wilson offered to sell—and Brantley agreed to buy—specific land for $ 370,000, cash price in full at closing, with closing costs to be split. They might also deduce, from Wilson's February 20 e-mail, that she later changed her mind about a previous decision to enter into a contract to sell, because she had been told she could get more money. Thus the Court concludes that there is a genuine issue of material fact as to whether objective indicators showed a meeting of the minds of Wilson and Brantley as to the sale of the Property.[124]

Cortez recognized that consent to participate in an electronic transaction may be judged from the surrounding circumstances. In that case, former employees brought a class action against the employer for labor law violations. The court granted a motion to compel arbitration, even though the employees denied signing an arbitration agreement. The employer, however, presented evidence that the employees agreed to submit disputes to arbitration by clicking buttons saying "I agree" to the arbitration clause. That click, the court held, rendered the agreement enforceable in light of the UETA. Explaining that "[w]hether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct."[125] the court pointed out that the evidence demonstrated that the employees agreed to enter into the agreement by electronic means:

> The argument is not convincing. The evidence shows that the software through which employees were asked

[124] *Brantley*, 2006 WL 436121 at *5-6.

[125] Cortez v. Ross Dress for Less, Inc., No. EDCV 13-01298 DDP, 2014 WL 1401869 at *3 (C.D. Cal. 2014) (citing CAL. CIV. CODE § 1633.5).

> to sign the DRA made explicitly clear, in understandable language, both before and after presenting the text of the DRA, that by clicking "I agree," the employees were entering into a binding agreement that disputes arising from their employment would be resolved by arbitration rather than by a court or jury. These circumstances satisfy the requirements for the creation of a valid contract under § 1633.5.[126]

Cases allowing the introduction of circumstantial evidence to prove an agreement to enter into electronic transactions involve affirmative action by both parties. The plain terms of Insuring Agreement (E) confirms that the parties (insured and insurer) did not consent to coverage for digital loan transactions and thus, absent an amendment to Insuring Agreement (E), the failure to procure the original document should preclude coverage.

B. Enforceability of .PDF Copies

Lenders commonly have reservations about using electronic records and signatures due to potential claims of unauthorized signatures and later discovery of forgeries. Section 9 of the UETA provides that:

> An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.
>
> The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.[127]

---

[126] *Id.* at *9.
[127] UETA § 9.

As noted above, UETA provides for "security procedures" which allow for a broad mechanism to demonstrate attribution:

> a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.[128]

The official comments further elaborate on this mechanism and its purpose, noting that a party may institute any security procedure to demonstrate attribution of a signature, and the use of a security procedure is merely one method, among others, by which a party might prove the source or content of an electronic record or electronic signature.[129] To mitigate against attribution risks generally, and particularly with respect to completely electronically closed transactions, parties must institute security procedures, such as:

- Initial face-to-face meetings between the parties at their business premises;
- Retention of emails associated with closings, signature releases and circulation of drafts and signed closing documents;
- Pre-closing calls with all parties verified on the call to confirm documents are final and conditions satisfied;
- FaceTime or other video conference service; and
- Conference call services that track parties dialed into the call.

While reminiscent of a traditional loan closing, such security procedures remain a critical component of reasonable lending procedures

[128] *Id.* at § 2(14).
[129] *Id.* at § 2, cmt. 11.

because an electronic record or electronic signature is attributable to a person if it was the act of the person. The act of a person may be shown in any manner, including the showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable. Accordingly, many banks adopt a "dual-tracked" closing wherein the parties exchange emailed PDF documents and follow-up wet signatures (with emails confirming that signatures are released after a final closing call), as such a procedure provides additional verification.[130]

The existing laws do not, however, contemplate the treatment of a scanned document as an original or as an electronic record. On the contrary, both the UETA and E-Sign contain express exceptions for transactions involving negotiable instruments. For example, E-Sign provides that it "shall not apply to a contract or other record to the extent it is governed by . . . . the Uniform Commercial Code in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A."[131] The UETA contains an analogous exception, stating that it "does not apply to a transaction to the extent it is governed by … the Uniform Commercial Code in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A."[132]

UCC Article 3 requires that negotiable instruments be in writing and be signed in ink since a "promise" is defined as a "written undertaking to pay money"[133] and a "writing" is defined as a "printing, typewriting, or any other intentional reduction to tangible form."[134] The question is whether a bank may obtain a handwritten promissory note, but then accept a scanned copy. UCC Article 3 was designed around the practice of possession and endorsement of a paper instrument and the

[130] Authenticating an electronic signature for evidentiary purposes follows roughly the same procedure as that for paper signatures, and as noted above, possible methods might include: a description of security procedures; certificates, affidavits or testimony from third-party providers; entry of personal information on a form; entry into evidence of metadata that identifies parties and their actions; and email correspondence between certain email addresses.

[131] 15 U.S.C. § 7003(a) (2000).

[132] UETA § 3(b).

[133] UCC § 3-103(a)(12).

[134] *Id.* § 1-201(b)(43).

rights and obligations that follow possession and endorsement. To further facilitate electronic transactions, ESIGN and UETA provide for the creation and existence of an electronic negotiable instruments—referred to a "transferable record."[135]

However, neither ESIGN nor the UETA provide carte blanche approval for all electronic records. An electronic promissory note intended to have the benefits of being a transferable record (carrying with it many of the rights granted a holder in due course under UCC Article 3) can only be created if the maker expressly agrees within the terms of such "electronic promissory note" that the same is issued as a transferable record. Transferrable records may not be created by the scanning of an inked promissory note:

> [C]onversion of a paper note issued as such would not be possible because the issuer would not be the issuer, in such a case, of an electronic record. The purpose of such a restriction is to assure that transferable records can only be created at the time of issuance by the obligor. The possibility that a paper note might be converted to an electronic record and then intentionally destroyed, and the effect of such action, was not intended to be covered by Section 16.[136]

The UETA provides protection for electronic notes, but only if the notes qualify as a "transferrable record"—defined as:

> (A) would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;
> (B) the issuer of the electronic record expressly has agreed is a transferable record; and
> (C) relates to a loan secured by real property.

[135] UETA § 16; 15 U.S.C. § 7021.
[136] UETA § 16 cmt. 2.

> A transferable record may be executed using an electronic signature.[137]

While the UETA adopts a facially broad definition of "transferrable record", the UETA then differentiates between copies exchanged electronically and true digital records by limiting legal rights and protection to a person exercising "control" over such records:

> Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in [Section 1-201(20) of the Uniform Commercial Code], of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under [the Uniform Commercial Code], including, if the applicable statutory requirements under [Section 3-302(a), 7-501, or 9-308 of the Uniform Commercial Code] are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively. Delivery, possession, and indorsement are not required to obtain or exercise any of the rights under this subsection.[138]

Proof of "control" therefore dictates the enforceability of an electronic note. The UETA imposes strict requirements for proof of control:

> A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.[139]

In order to qualify as a transferable record, a note must be electronically created, presented to the borrower and executed entirely on information processing systems, and:

---

[137] UETA § 16(a); *see also* 15 U.S.C. § 702(a)(1).
[138] UETA § 16(d).
[139] *Id.* §16(b).

- The note otherwise qualifies as a negotiable promissory note under Article 3 if it were in writing.

- The issuer (the borrower) expressly agree that the instrument is a transferable record.

- The method used to record, register, or evidence a transfer of interests in the note must reliably establish the identity of the person entitled to "control" the note.[140]

Unless all of these criteria are met, the person identified as the controller obtains rights equivalent to those granted a holder of a paper promissory note, which includes the right to enforce the note.

The UETA provides a safe harbor for satisfying the rules establishing control.[141] Under the safe harbor provisions, the transferable record must be created, stored, and assigned so that the following conditions are met:

> (c) Conditions: A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that—
> (1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;
> (2) the authoritative copy identifies the person asserting control as—
> (A) the person to which the transferable record was issued; or
> (B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

[140] *Id.*
[141] *Id.* §16 cmt. 3.

> (3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
> (4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;
> (5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and
> (6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.[142]

Such a standard effectively limits the scope of a transferrable record to a unique and unalterable document created electronically because it requires:

- A single authoritative copy of the record exists that is unique, identifiable, and (except for permitted revisions under UETA), unalterable;
- The authoritative copy identifies the person asserting control as either the person to whom the Transferable Record was issued or the person to whom the Transferable Record was most recently transferred;
- The authoritative copy is communicated to and maintained by the person asserting control or his designated custodian;
- Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;
- Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

[142] *Id.* at § 16(c).

- Any revision of the authoritative copy is readily identifiable as an authorized or unauthorized revision.

Courts to date have used this general rule.[143] *Good v. Wells Fargo*[144] is the first reported decision to directly address ownership and enforcement of an e-note. In *Good*, Wells Fargo sought to enforce a debt evidenced by an e-note governed by the provisions of E-SIGN (because the e-note was secured by real property). However, the affidavits supporting Wells Fargo's motion did not provide any evidence on the question of "control." The district court granted Wells Fargo partial summary judgment, finding that Wells Fargo had standing to enforce the promissory note. The debtor appealed.

The Indiana Court of Appeals reversed and remanded for further proceedings. The court held that because the e-note was secured by real property, issues related to "control" were governed by E-SIGN. The court went on to find that in order to enforce the e-note, Wells Fargo needed to show that it controlled the e-notes of the date the foreclosure action was filed, and had not done so because it had failed to present any evidence supporting its claim to control.[145] The court observed that under the terms of the e-note itself, control and location of the authoritative copy were to be determined by reference to a note holder registry, and that Wells Fargo had not provided any evidence of entries in a note holder registry establishing that it was the party in control.

However, the court also held that Wells Fargo was correct that pursuant to E-SIGN, "a person having control of a transferable record,

[143] Courts have emphasized that the plaintiff bringing a foreclosure action on a note must present competent evidence that the plaintiff was in control of the eNote on the date the action was filed. *See* Wells Fargo Bank, N.A. v. Benitez, No. 13-15433, slip op 32564(U) (N.Y. App. Div. 2016) (plaintiff seeking to enforce an e-note must provide evidence that a system employed for evidencing the transfer of interests in the e-note reliably establishes that control has been transferred to the plaintiff); Bank of N.Y. Mellon Trust Co., N.A. v. Carpenter, Index N0. 701473/2015 (N.Y. Sup. Ct. 2017) (where the evidence showed that a party other than the plaintiff had control of the e-note on the date the foreclosure action was filed, the plaintiff failed to establish standing to bring the foreclosure action).

[144] 18 N.E.3d 618 (Ind. App. 2014).

[145] *Id.* at 623-24.

which includes the Note, is the holder for purposes of the UCC and that delivery, possession, and endorsement are not required."[146] To show it controlled the note, Wells Fargo was required to designate evidence that "a system employed for evidencing the transfer of interests in the Note reliably established Wells Fargo as the person to whom the Note was transferred."[147]

Two later reported decisions pick up the *Good* decision and confirm its view of the requirements for establishing control and the rights of the controller. On April 13, 2015, a New York appellate court, in *New York Community Bank v. McClendon*, issued an opinion reversing a lower court order dismissing a foreclosure action against a borrower who signed an e-note.[148] In the proceedings below, the lower court had granted the borrower's motion to dismiss because the plaintiff could not produce a chain of valid assignments of the e-note from the original lender to itself. However, the mortgagee had submitted in evidence a copy of the e-note and a print out of an electronic record of the transfer history of the e-note on the MERS eRegistry showing a chain of transfers from the original lender to itself. The appellate court concluded that the transfer history, together with the e-note, were sufficient to establish that the plaintiff mortgagee had control of the e-note under ESIGN and therefore had standing to foreclose as the holder:

> Here, the eNote transfer history established that the eNote was transferred by the FDIC, as receiver for AmTrust Bank, to the plaintiff on March 23, 2010, more than two years before the plaintiff commenced the instant action on or about June 18, 2012. The transfer history further established that, on March 23, 2010, the plaintiff obtained control and became the owner of the eNote. Thus, the transfer history, together with the copy of the eNote itself, were sufficient "to review the terms of the transferable record and to establish the identity of the person [or entity] having control of the transferable record" (15 USC § 7021 [f]). This evidence was sufficient to establish the plaintiff's standing as the

[146] *Id.*
[147] *Id.*
[148] 29 N.Y.S.3d 507 (N.Y. App. Div. 2016).

> holder of the eNote and rendered the lack of proof of valid assignment irrelevant.[149]

In the second case, a Florida court of appeals issued an opinion in *Rivera v. Wells Fargo Bank, N.A.*[150] affirming judgment against borrowers who signed an e-note. In the proceedings below, the bank presented a sworn certificate of authentication which articulated, among other things, the bank's role as servicer of the e-note for Fannie Mae, and described the bank's practices and systems used for the receipt and storage of authoritative copies of electronic records and for protecting electronic records against alteration. The bank also provided evidence from the same system records, and the records of the MERS eRegistry showing that the e-note was last transferred to Fannie Mae and that the authoritative copy of the e-note was maintained in the bank's systems as Fannie Mae's custodian.

On appeal, the borrowers challenged the adequacy of the bank's demonstration that the e-note had properly transferred to Fannie Mae. Applying the Florida enactment of the UETA and relying on the evidence provided in the certificate of authentication, the court held that the bank presented competent evidence proving that Fannie Mae owned the e-note and authorized the bank to pursue the foreclosure:

> The e-note, on its face, is a "transferable record" because it is an electronic record that would be a note under chapter 673 if it were in writing, and its issuer expressly agreed on its face that it was a transferable record. § 668.50(16)(a). . . . According to the bank's evidence, the bank's system stored the e-note in such a manner that a single authoritative copy of the e-note exists which is unique, identifiable, and unalterable. § 668.50(16)(c)(1). That authoritative copy, introduced into evidence by the bank as Fannie Mae's designated custodian, identified Fannie Mae as the entity to which the transferable record was most recently transferred. . . .[151]

---

[149] *Id.* at 509-10.
[150] 189 So. 3d 323 (Fla. Dist. Ct. App. 2016).
[151] *Id.* at 329.

Rivera demonstrates the distinction between a true transferrable record and a scanned copy of an ink signed document. A scanned version is not a unique and unalterable document; it represents a copy of an original document. Thus, a financial seeking to enforce a digital record cannot rely upon a scanned copy, but instead must demonstrate the digital creation of the document and the maintenance of such document in a format ensuring that it was and remains unique, identifiable, and unalterable.

V.
RISK ANALYSIS UNDERLYING THE SELECTIONS OF AN ELECTRONIC SIGNATURE SOLUTION

Electronic signatures have existed for as long as the technology used to record them. As early as 1867, courts recognized a telegraphed signature to satisfy the Statute of Frauds.[152] As new technologies were invented, courts followed by recognizing the legal validity of signatures

[152] Trevor v. Wood, 36 N.Y. 307, 310 (N.Y. 1867); *see also* Howley v. Whipple, 48 N.H. 487, 488 (N.H. 1869) ("It makes no difference whether that operator writes the offer or the acceptance. . .with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office."). For a general account of the history of signatures, see generally CHRIS HAWKINS, A HISTORY OF SIGNATURES: FROM CAVE PAINTINGS TO ROBO-SIGNINGS (2011). For a history on the Statute of Frauds with regard to advances in technology, see Steven Domanowski, *E-SIGN: Paperless Transactions in the New Millennium*, 51 DEPAUL L. REV. 619, 622-36 (2001).

communicated by telephone to an operator,[153] via tape recordings of an oral agreement,[154] and by facsimile.[155]

Today, the use of electronic signatures in commercial transactions has exploded with the advent of computer technology. With ever-developing advances in hardware and software, the forms that an electronic signature can take are also constantly evolving. Initially, electronic data interchange emerged as a means for communicating standardized forms such as purchase orders, invoices, and shipping notices between two businesses irrespective of the particular hardware or software implemented at either end of the transmission.[156] This method effectively communicated between businesses, enabling them to establish trade relationships as they could sign traditional paper agreements governing the exchange of electronic messages between themselves.[157]

Digital signatures do not look like traditional signatures and are better understood as a "signature by process to the document." Most methods of creating an e-signature involve a technology, credentials or digital objects. Each approach varies in terms of the level of certainty, attribution and security. A proper e-signature protocol focuses to ensure sufficient process to verify signer identification and signature attestation.

---

[153] Selma Sav. Bank v. Webster Cty. Bank, 206 S.W. 870, 874 (Ky. 1918) (holding that a contract is formed when a telephone message is transmitted to a telegraph operator).

[154] Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 1228 (D. Colo. 1972) (holding that a tape recording of an oral agreement satisfies the statute of frauds). *But see* Swink & Co. v. Carroll McEntee & McGinley, Inc., 584 S.W.2d 393 (Ark. 1979) (holding that a tape recording may satisfy the writing requirement but not the signature requirement).

[155] Vazak Intl. Corp. v. Mast Indus., 535 N.E.2d 633 (N.Y. 1989); Hessenthaler v. Farzin, 564 A.2d 990 (Pa. Super. Ct. 1989).

[156] Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange - A Report and Model Trading Partner Agreement*, 45 Bus. Law. 1645, 1649-51 (June 1990). For a helpful description of EDI technology, *see also* R.J. Roberston, Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998).

[157] See Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA*, 56 BUS. LAW. 293, 294-97 (2000).

Signer Identification refers to the policy, process and procedures used to authenticate the signer and thereby establish a link or association between the signer and the information and method used to sign. A proper e-signature requires a process to identify and authorize an individual to use a particular e-signature application. The more robust or stringent the identification method, the more assurance that the signature has been used by the person who he or she purports to be. This can help protect against fraud and repudiation.

Signature attestation refers to the ability of an e-signature to protect against unauthorized access or tampering with the signed e-record and therefore reduce the risk of intrusion, inadvertent disclosure, fraud, and repudiation. This protection can be achieved by the system that collectively manages the e-record and the associated e-signature. In such a case, the key factor is the system's trustworthiness and its controls to ensure that a record or signature has not been tampered with or modified, as well as the system's ability to detect if that has occurred.

Role of Signer: Important information used to create and authenticate e-signatures requires a high-level of security. Regardless of signature approach, the role of the signer is critical to securing e-signature information. Information used to create an e-signature should be under the sole control of the signer. Therefore, a key component of the security of e-signatures is dependent on the signer's behavior.

Selecting an e-signature solution involves more than technical considerations. This business analysis and risk assessment requires an institution to identify and evaluate various factors—including the relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process.

Critically, a business must assess the risk of permitting e-signatures. E-signatures should serve a security function as well as a legal purpose. Proper e-signature processes include authentication of the signer, or another security feature such as message authentication and repudiation protection. Therefore, the selection of an appropriate e-signature solution includes identifying the potential legal, security and

technological risks involved in a signed electronic transaction and how various e-signature approaches can address those risks.

Risk is a function of the likelihood that a given threat will exploit a potential vulnerability and have an adverse impact on an organization. Threats to electronic transactions can come from parties to the transaction, or malicious third parties such as hackers or crackers. A threat can be an intentional act, such as a deliberate attack by a malicious person or disgruntled employee, or an unintentional act, such as negligence and error. In assessing the sources of threats, it is important to consider all potential entities that could cause harm or disrupt a transaction.

Thus, a business should identify and analyze vulnerabilities. Those potential vulnerabilities including repudiation (*i.e.*, the possibility that a party to a transaction denies that the transaction ever took place) due to fraud, a misunderstanding or a difference in interpretation; fraud (*i.e.*, a knowing misrepresentation of the truth or concealment of facts to induce another to act to his or her detriment); intrusion (*i.e.*, the possibility that a third party intercepts or interferes with a transaction).[158]

Such vulnerabilities often depend upon the motivation and capability of the source of the threat, the nature of the vulnerability, and existence and effectiveness of current controls. A threat is highly likely where its source is highly motivated and capable and controls are ineffective. A threat is less likely where the source lacks motivation or capability and effective controls can prevent or significantly impede the threat. Recognizing this distinction, a company can adopt different e-signature solutions depending upon the risk:

- ***Low risk***: Some organizations use e-signatures for everyday business agreements such as contracts, statements of work, or employee forms. Using a secure login process, the signer receives an email containing an

[158] The probability of an intrusion can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. Regular or periodic transactions are more vulnerable than intermittent ones because they are predictable and it is more likely that an outside party would know they are scheduled and be prepared to intrude on them.

link granting access the document. This process securely manages the document execution process, and creates an audit trail. Upon final execution, the final document is transmitted with a seal to confirm its integrity.[159]

- ***Moderate risk***: To strengthen security, a company can add multi-factor authentication. Such practices operate like standard e-signatures, but add a signer authentication (such as phone PINs, social IDs, passwords, or knowledge-based authentication), to provide a heightened level of signor verification.[160]

- ***High risk***: To meet the most stringent legal compliance and protect the signing processes, most organizations choose digital signatures.[161]

Given the varying uses, electronic signature solutions run the gamut from "barebones" services to complete business solutions for managing documents, signatures, secure storage, reporting, legal defense, administrative controls, and workflow management. The following are examples of common electronic signature solutions, highlighting their strengths and weaknesses.

Click Through: This method creates a legally binding agreement by requiring the user to click "I Agree" to an agreement or otherwise exhibit that they explicitly agree in some way. In some instances, the user will be required to affirmatively check a box at the end of their web form saying "I agree to the terms and conditions."[162] The enforceability

[159] *Get Set for E-signature Success. Developing an Effective Electronic Signature Policy* (2017), https://acrobat.adobe.com/content/.../wp-document-cloud-esignature-policy-ue.pdf.

[160] *Id.*

[161] *Create an electronic signature policy*, https://www.foxitsoftware.com/blog/create-an-electronic-signature-policy/; *Developing an effective electronic signature policy*, https://blogs.adobe.com/documentcloud/developing-an-effective-electronic-signature-policy/.

[162] Leah, *3 Key Legal Cases on Click-wrap*, TERMS FEED (Oct. 23, 2016), https://termsfeed.com/blog/3-key-legal-cases-on-click-wrap/. Low risk, low value consumer transactions often adopt this approach. It can be combined

of this method often depends upon the exact language used and whether the user is adequately forewarned and conspicuously affirms assent.[163]

Personal Identification Number or Password: When using a PIN or password for an e-signature, a person accessing an application is requested to enter identifying information, which may include an identification number, the person's name and a "shared secret" (called "shared" because it is known to both the user and the system), such as a PIN and/or password. The system checks that the PIN and/or password is indeed associated with the person accessing the system and "authenticates" the person.

The identification and verification process used to issue a PIN and/or password varies depending on the level of security deemed necessary and the assumed risk or value of a transaction. For low risk or low value transactions, the person may define a PIN and/or password after supplying minimal identifying information that may or may not be verified. For higher risk transactions, the PIN may be issued by the organization sponsoring the application after an identification process requiring substantial personal information and rigorous verification procedures.

The entropy of the password can provide additional security. The higher the entropy, the more difficult the password is to guess or crack using hacker techniques. Medium and high-risk transactions often require a hardened password consisting of a combination of letters, alphanumeric numbers, and special symbols at least eight (8) characters in length. The user might be forced to authenticate using a security token or digital certificate and a second password different than the one that they log on with for accessing enterprise low-risk systems, applications and information.

---

with use of a Personal Identification Numbers (PINs) and/or passwords to authenticate signers to provide greater security.

[163] Specht v. Netscape, 306 F.3d 17 (2d Cir. 2002) (absence of a conspicuous act reflecting assent precluded enforcement of the agreement); Feldman v. Google, Inc., 513 F. Supp. 2d 229 (E.D. Pa. 2007) ("[t]o determine whether a clickwrap agreement is enforceable, courts presented with the issue apply traditional principles of contract law and focus on whether the plaintiffs had reasonable notice of and manifested assent to the clickwrap agreement.").

Digitized Signature: A digitized signature is a graphical image of a handwritten signature.[164] These types of signatures might look official, but they do not offer security against tampering, a critical element of any online signature.[165]

> The obvious risk is that typed signatures, email footers and scanned signatures can so easily be copied or forged that it cannot be long before a serious financial dispute arises in which one party alleges that the "signature" was not applied by them, or that the document was altered after being signed. . . There is massive scope for dispute even if the forgery is proven, as both parties are likely to have acted in reliance on the forged agreement.[166]

To increase security, some applications require a person to create a handwritten signature using a special computer input device (such as a digital pen and pad) or use an application to compare the digitized representation of the signature with a stored copy of the graphical image of the signature.[167]

Signature Dynamics: This is a variation on a digitized signature in which each pen stroke is measured (e.g., duration, pen pressure, size of loops, etc.), thereby creating a metric. This metric can also be compared to a reference value created earlier, thus authenticating the person who applied the signature. The signature dynamics measurements can be combined with techniques used to create a digital signature (see

---

[164] Emily Maxie, *Digitized Signatures v. Digital Signatures: A Complete Comparison*, SIGNIX BLOG (JULY 25, 2013), https://www.signix.com/blog/bid/99443/Digitized-Signatures-vs-Digital-Signatures-A-Complete-Comparison.

[165] *Id.* Digitized signatures are most often used in face-to-face consumer transactions using credit cards. In such cases the signature is rarely validated.

[166] *Id.*

[167] This approach shares the same security issues as those using the PIN or password, because the digitized signature is another form of shared secret known both to the person and to the system. Forging a digitized signature can be more difficult than forging a paper signature because the technology that compares the submitted signature image with the known signature image is more accurate than the human eye.

below) to ensure document integrity and a more reliable authentication of the signer.[168]

Biometrics: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. In this approach, the physical characteristic (*i.e.*, voice patterns, fingerprints, face recognition, DNA, palm print, gait analysis, hand geometry, and retinal and iris recognition) is measured and converted into a digital form or profile. These measurements are compared to a profile of the given biometric stored in the computer and authenticated beforehand as belonging to a particular person. If the measurements and the previously stored profile match, the software will accept the authentication, and the transaction is allowed to proceed.[169]

Shared Private Key Cryptography: Shared key encryption uses one key to encrypt and decrypt messages. For shared key cryptography to work, the sender and the recipient of a message must both have the same key, which they must keep secret from everybody else. The sender uses the shared key to encrypt a message and then sends the ciphertext message to the recipient.[170]

---

[168] *The usage of handwritten dynamic (biometric) signatures in the digital world—and its implications*, FIND BIOMETRICS (Nov. 14, 2007), https://findbiometrics.com/the-usage-of-handwritten-dynamic-biometric-signatures-in-the-digital-world-and-its-implications/. A proper comparison of static signature characteristics and dynamic signature signals requires a digitizing instrument able to differentiate between various pressure levels and to provide an appropriate resolution rate. (ISO/IEC FDIS 19794-7).

[169] Danny Thakkar, *Identity Goes Digital with Biometric Signature Verification*, BAYOMETRIC BLOG, https://www.bayometric.com/biometric-signature-verification/ (last visited June 5, 2018); Find Biometrics, *supra* note 168.

[170] A common and secure use of symmetric encryption for authentication is a one-time password token (e.g. RSA SecureID). This is a small secured hardware device where the symmetric key generates "one time" passwords every few minutes. The one-time password typically is displayed on the device and is inputted from the device to a computer, usually along with a PIN. https://www.cryptomathic.com/news-events/blog/what-is-an-electronic-signature-policy.

Public/Private Key Cryptography: Public key encryption uses a pair of complementary keys (a public key and a private key) to encrypt and decrypt messages. The two keys are mathematically related such that a message encoded with one key can only be decoded with the other key. Although a user's public and private keys are mathematically related, knowledge of a public key does not make it possible to calculate the corresponding private key.[171]

Private keys offer significant benefits in terms of authentication, non-repudiation, and integrity. Absent disclosure, the key increases authentication (since the individual uses a unique private key to apply the signature, thus enabling recipients to be more confident that the individual was the one to actually apply the signature), reduces the risk of non-repudiation (since the individual is the only one with access to the private key used to apply the signature, he/she cannot later claim that it wasn't him/her who applied the signature), and increases integrity (as even the slightest change to the original document would cause this check to fail).[172]

Digital signatures protected by a public-key infrastructure "are widely recognized as best practice for ensuring digital accountability for electronic transactions."[173] Support from a public-key infrastructure provides trustworthy indicia of the signor's identity, protection against

[171] Francis Knott, *What is Private Key Encryption?* KOOLSPAN, https://koolspan.com/private-key-encryption/ (last visited June 5, 2018). The public key is often made part of a "digital certificate," which is a digitally signed electronic document binding the individual's identity to a private key in an unalterable fashion. A "digital signature" is created when the signer uses the private signing key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document employs the signer's public key to validate the authenticity of the attached private key and to verify that the document was not altered subsequent to signing.

[172] *What is Public-key Cryptography?* GLOBALSIGN, https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/ (last visited June 5, 2018).

[173] *Digital Signatures—Best Practice for e-Business Transactions*, https://www.entrust.com/wp-content/uploads/2013/05/digsig_transactions.pdf (last visited June 5, 2018).

forgery, protection from subsequent alteration and compliance with UETA/E-Sign.[174]

VI.
CONCLUSION

While the continued evolution of digital technology, financial institutions will continue to explore the implementation of electronic lending and security over such transactions. While not currently within the scope of a financial institution bond, the increase of electronic transactions provide an opportunity to advanced security features and whether the implementation of such procedures enhances the insurability of such transactions.

[174] *Id.*