ELECTRONIC SIGNATURES IN AGRICULTURE: LAW, GUIDELINES, AND RECOMMENDATIONS

*John Hughes, Sangramsinh Shinde, & John L. Brown**

Note: The views expressed in this article are those of the authors and do not necessarily reflect those of Deere & Company or any of its affiliates.

I. INTRODUCTION

Today's farmers are just as likely to mention smartphones and tablet computers as they are seed, fertilizer, and crop protectants as integral tools for their success.[1] Farmers, from those who operate on a few acres to those with thousands, rely on smartphones for timely communication. As they measure cost-per-acre and crop yields, farmers consult productivity reports on tablet computers in the farmhouse as well as in the field.[2] In concert with smartphones and tablet computers, GPS technology enables farmers to track the locations of their machines and manage their equipment fleet.[3]

---

*John Hughes, J.D. University of Iowa, 2002; B.A. Summa Cum Laude in Human Resource Management with a minor in Business Communication, Purple and Old Gold Award, University of Northern Iowa, 1999; licensed to practice law IA;

Sangramsinh Shinde, Masters of Law Specialty in Law of Contracts University of Pune, I.L.S. Law College University of Pune, John Deere Global Law Services Group, Legal support services, Compliance audit, and Contract Management;

John L. Brown, J.D. with honors University of Iowa College of Law 1980, B.A. Economics and Political Science, Northwestern University 1977, Associate Lucas, Brown & McDonald 1980-1983, Assistant Vice President ITT Consumer Financial Corporation 1983, Associate Chief Counsel Deere Credit Services, Inc. 1983-Present, Designated John Deere Fellow in 2015, licensed to practice law in IA, IL, MN, and WI, Published in Journal of Bankruptcy Law & Practice, Consumer Finance Law Quarterly Report, and Drake Journal of Agricultural Law.

[1] Ben Potter, *87% of Farmers Will Own a Smartphone by 2016*, AGWEB (Jan. 25, 2016), http://www.agweb.com/article/87-of-farmers-will-own-a-smartphone-by-2016-naa-ben-potter/ (discussing the findings of an online survey which projected that 87% of farmers will own smartphones and 59% will own tablet computers by 2016).

[2] *See generally* John Dietz, *Farm Apps*, SUCCESSFUL FARMING (Feb. 5, 2013), http://www.agriculture.com/farm-management/technology/cell-phone-and-smart-phones/farm-apps_325-ar29465.

Similar to farmers, equipment dealers and agribusiness merchants are also leveraging technology. The recent consolidation within the dealer and agribusiness sectors has served to accelerate the use of technology for efficiencies.[4] Nearly 70 percent of agribusiness sales representatives surveyed by the industry publication *CropLife* now use tablet computers as part of their daily work. Doing so provides agribusiness merchants with precise agriculture readouts, which allows them to pinpoint crop concerns and provide more valuable feedback to their customers. Equipment dealers, who may be as far as four hours away from their customers, can collect remote service information electronically to diagnose equipment performance issues.

Financial service providers, who help farmers, dealers, and merchants complete sales, also embrace technology. Specifically, electronic contracts (e-contracts) and signatures are representative of how some financial service providers are using technology to facilitate commerce. Tablet computers that store e-contracts for signatures allow dealer salespersons to forego carrying lengthy paper contracts. Dealers submitting many contracts to financial service providers for booking can now send them electronically and cut postage expenses. Additionally, financial service providers that receive over a thousand installment contracts for booking each day during peak business cycles can receive and store electronic signature documents without having to manage piles of paper.

While e-contracts and signatures bring benefits for those in the agricultural finance industry, the technology raises a potential legal issue of contract enforceability with respect to remotely-signed documents: How does the law treat farmer-customers who challenge the validity of e-contracts presented via means where the dealer, merchant, or lender is not present to witness the customer signature? Common substitutes for the lender actually witnessing the customer's signature include electronic documents exchanged via email and website portals

---

[3] *See generally Technologically Advanced Ag Tools for the 21st Century*, FARM FORUM (Jan. 4, 2013), http://www.farmforum.net/2013/01/04/technologically-advanced-ag-tools-for-the-21st-century/.

[4] Eric Sfiligoj, *Cooperative Consolidation Continues*, CROPLIFE (Nov. 16, 2015), http://www.croplife.com/editorial/cooperative-consolidation-continues/.

that ask security questions before customers may proceed with their electronic signature.

Equipment dealer and agribusiness merchant personnel potentially avoid enforceability issues today when they witness the farmer-customer's electronic signature on a tablet computer at the farm or in a salesperson's office. However, the increasing distance between some farmers and their equipment and input providers adds costs such as fuel and travel time to these in-person signature events. Appointments for in-person signature events are also less convenient than conducting electronic commerce, which can occur at any time of day. Remote electronic-signature solutions that help parties reduce travel expenses and increase convenience while maintaining contract enforceability therefore bring value.

This article explores the statutes, case law, and practical issues that relate to enforcing remotely-signed e-contracts within commercial agriculture lending. Throughout this article, attention is devoted to knowledge-based authentication as a particular method for validating remotely-signed e-contracts. Finally, this article will offer conclusions on what constitutes sufficient knowledge-based authentication for remotely-signed e-contracts and how that authentication affects the burdens of proof in challenging them.

II. U.S. ELECTRONIC SIGNATURE STATUTES: FEDERAL ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT AND STATE UNIFORM ELECTRONIC TRANSACTIONS ACT

With the ease, security, and benefits that technology offers, companies—especially in the financial sector—started leveraging electronic signatures to accelerate and expand business transactions. It is, however, important to note that simply placing a symbol on a document does not by itself create an enforceable contract. For the contract to be valid and enforceable, it is essential that electronic signatures are accepted as legally binding.

There are two acts that ensure the legality of documents executed with electronic signatures in the United States: the Federal Electronic Signatures in Global and National Commerce

Act ("E-SIGN") and, at the state level, the Uniform Electronic Transactions Act ("UETA").[5]

Both E-SIGN and UETA establish that electronic signatures and electronic records carry the same weight and legal effect as handwritten signatures and traditional paper documents.[6] E-SIGN and UETA generally provide the following: (1) a signature, contract or record may not be denied legal effect or enforceability solely because it is in electronic form; (2) a contract may not be denied legal effect or enforceability solely because an electronic signature or electronic record was used in its formation; (3) if a law requires a signature, an electronic signature satisfies the law; and (4) if a law requires a record to be in writing, an electronic record satisfies the law.[7]

However, for electronic signatures to enjoy the same legally binding status as those that are handwritten, almost all documents signed between parties in the United States must meet the requirements provided by E-SIGN and UETA:

> Intent to Sign – Electronic signature, like traditional wet ink signature, is valid only if the signer intends to sign the document and there is no possibility of forgery.[8]
>
> Consent to Do Business Electronically – In Business-to-Consumer dealings, where customers may not always be clear what they are signing and why, electronic records may be used in transactions only if the consumer has affirmatively consented to use electronic records for the transaction[9] and has not withdrawn such consent.[10]

---

[5] *See generally* 15 U.S.C.S. § 7001 (Lexis through Pub. L. No. 115-22); UNIF. ELECTRONIC TRANSACTION ACT (1999).

[6] *Id.*; UNIF. ELECTRONIC TRANSACTION ACT (1999).

[7] 15 U.S.C.S. § 7001(a)(1)(2) (Lexis through Pub. L. No. 115-22); UNIF. ELECTRONIC TRANSACTION ACT § 7(a)-(d) (1999).

[8] 15 U.S.C.S. § 7006(5) (Lexis through Pub. L. No. 115-22); UNIF. ELECTRONIC TRANSACTION ACT § 2(8) (1999).

[9] 15 U.S.C.S. § 7006(13) (Lexis through Pub. L. 115-22) (defining transaction as 'action relating to conduct of business, consumer or commercial affairs between two or more persons and includes sale, lease or other disposition of personal property (goods & intangibles), services and its combination'); UNIF. ELECTRONIC TRANSACTION ACT § 2(16)

> Consumer Disclosure – Prior to obtaining consent, financial institutions must provide the consumer a clear and conspicuous statement informing the consumer (1) of (a) any right or option to have record provided or made available on paper or in non-electronic form; and (II) right to withdraw such consent and any conditions, consequences (which may include termination of parties' relationship) or fees in event of withdrawal; (ii) whether consent applies (I) only to particular transactions which give rise to obligation to provide record; or (II) to all identified categories of records that may be provided or made available during course of parties' relationship; (iii) of procedures to use to withdraw consent and to update information needed to contact consumer electronically; (iv) (I) how, after consenting, and upon request, a paper copy of electronic record may be obtained; and (II) whether any fee will be charged for such copy; and (v) of hardware and software requirements for access to and retention of electronic records.[11]
>
> Signature Must Be Associated with Record – 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.[12]
>
> Record Retention and Access to Records – Electronically signed documents are valid only if

---

(1999) (defining transaction as 'action occurring between two or more persons relating to conduct of business, commercial or governmental affairs').

[10] 15 U.S.C.S. § 7001(c)(1)(A) (Lexis through Pub. L. 115-22).

[11] 15 U.S.C.S. § 7001(c)(1)(B)(C) (Lexis through Pub. L. 115-22).

[12] 15 U.S.C.S. § 7006(5) (through PL 115-22); UNIF. ELECTRONIC TRANSACTION ACT § 2(8) (1999).

> they are capable of being retained and accurately reproduced (by transmission, printing or otherwise) for later reference by all parties to contract.[13]

Though comprehensive, E-SIGN and UETA do not apply to: (1) wills, codicils or testamentary trusts; (2) divorce matters; (3) certain areas of the Uniform Commercial Code; (4) court orders, notices or official court documents; (5) notice of cancellation of utility services; (6) notice of default, repossession, foreclosure, eviction; (7) notice of cancellation of health insurance benefits or life insurance benefits (excluding annuities); (8) notice of product recall or material failure; or (9) documentation accompanying the transportation/handling of hazardous materials, pesticides or other dangerous materials.[14]

III. LEGAL ISSUES OF CUSTOMER AUTHENTICATION AND ATTEMPTED REPUDIATION OF PAPER CONTRACTS

Courts address acts of forgery in paper contract transactions as well as those transactions with electronic signatures. The following section includes case illustrations where forgery was alleged for both paper and electronic signature transactions.

Iowa case law provides two examples of paper contract forgeries. In *Shea v. Cutler*, the Iowa Supreme Court deemed a paper contract with erasures and alterations, made without knowledge of the defendant, to be not binding where the defendant denied making the signature.[15] In another case, *Brien v. Davidson*, the Court found three altered paper contracts to be forgeries in an estate matter.[16]

Similarly, multiple courts have found that "electronically filing a document bearing an electronic signature that was not

---

[13] 15 U.S.C.S. § 7001(d)(1)(A)(B) (Lexis through Pub. L, 115-22); UNIF. ELECTRONIC TRANSACTION ACT § 8 (1999).

[14] 15 U.S.C.S. §103(a) (b) (Lexis through Pub. L. 115-22); UNIF. ELECTRONIC TRANSACTION ACT § 3 (1999).

[15] Shea v. Cutler, 126 N.W. 366, 368 (Iowa 1938).

[16] Brien v. Davidson, 281 N.W. 150, 151 (Iowa 1938).

actually or validly signed" constitutes a forgery.[17] In *In re Stomberg*, where an attorney forged his client's electronic signature, the court held that electronically filing a document that purports to have the client's signature but which was not, in fact, signed by the client, is no different than physically forging the client's signature on a paper document.[18]

A similar issue was considered in *In re Bradley*.[19] There, an attorney allowed his assistant attorney to forge their client's signature electronically.[20] The court held that authorizing the filing of defective pleadings with forged electronic signatures violated the law.[21] In *In re Flowers,* the court held that an attorney violated the law by forging the electronic signature of another attorney on bankruptcy petitions and other documents.[22]

IV. U.S. INK SIGNATURE ENHANCEMENT FOR PAPER CONTRACTS

As the previous section describes, courts have ruled on forgery in both paper and electronic transactions. Thus, signature authentication continues to be a key focus for judicial review. This section surveys pen and ink signature presumptions as well as proof of validity methods.

The law has evolved in many jurisdictions in response to parties disputing the validity of documents they allegedly signed. A notable example of this can be found in the Iowa Rules of Civil Procedure. There, where a proponent of a signed writing claims it was also signed by an adverse party, both signatures will be presumed valid unless the adverse party denies the genuineness of his or her signature.[23] The denial by the adverse party must be verified by that party.[24] If that is done, the burden of proving the validity of the contested signature shifts back to the proponent.[25]

---

[17] In re Bradley, 495 B.R. 747, 780 (Bankr. S.D. Tex. 2013).
[18] In re Stromberg, 487 B.R. 775, 808 (Bankr, S.D. Tex. 2013).
[19] *See generally Bradley*, 495 B.R. 747.
[20] *Id.*
[21] *Id.*
[22] In re Flowers, 2012 WL 987298 (Bankr. E.D.N.Y. Mar. 22, 2012).
[23] IOWA R. CIV. P. 1.405(4).
[24] *Id.*
[25] *Id.*

However, if the denial is not verified by the adverse party, the signature is deemed to be prima facie genuine.[26]

Proof that the contested signature is that of the adverse party can be established by testimony of: (1) persons familiar with the adverse party's signature; (2) those who witnessed the affixing of the adverse party's signature; and/or (3) of a handwriting expert.[27] The law also permits self-authentication; a process where a state appointee (e.g., a notary public or other officer authorized by law to take acknowledgements) writes, signs, and seals an acknowledgement (i.e., certificate) describing the signing event.[28] Generally, the acknowledgment recites that the alleged signer appeared before the state appointee, to be accurately identified, and notes that the signer acted voluntarily.[29] This self-authentication shifts the burden of proof to the adverse party, who then must prove the signature's lack of authenticity by a preponderance of the evidence. If the adverse party cannot do so, the signature will be deemed authentic.[30]

The trend toward less local business transactions has given rise to the signature guaranty product; that is, where the party witnessing the signature also guaranties that any signature challenged in U.S. courts will be found genuine. One common signature guaranty method is the securities transaction Medallion Signature Guarantee.[31] This program includes the STAMP (Securities Transfer Agent Medallion Program), SEMP (Stock Exchanges Medallion Program) and MSP (New York Stock Exchange Inc. Medallion Signature Program).[32] These guaranties are generally provided by federally or state chartered banks, savings associations, trust companies, broker-dealers, clearing agencies, and other financial institutions.[33] However, many of these entities will issue a signature guaranty only for one of their

---

[26] Quaas v. Quaas, 92 N.W.2d 427 (Iowa 1958).

[27] *See* IOWA CODE ANN. § 622.25 (West 2016); *See also* 8 IOWA PRACTICE, CIVIL LITIGATION HANDBOOK § 21:8 (2016).

[28] *See* 8 IOWA PRACTICE, CIVIL LITIGATION HANDBOOK § 40:4 (2016).

[29] *Id.*

[30] *See Quaas*, 92 N.W.2d at 432-33.

[31] *See generally Investing with Us*, U.S. GLOBAL INV. FUNDS, http://www.usfunds.com/investing-with-us/faqs/account-maintenance/what-is-a-medallion-signature-guarantee-and-where-can-i-obtain-one/ (last viewed Mar. 30, 2017).

[32] *Id.*

[33] *Id.*

customers and typically charge a fee for that service.[34] By affixing its Medallion guarantor stamp, the guarantor warrants that: (1) the accompanying signature is genuine; (2) the signer is an appropriate person to sign; and (3) the signer had the legal capacity to sign.[35] If any of these warranties are breached, the guarantor is liable for the resulting loss to any person taking or dealing with the security in reliance of the guarantee.[36] Signature guaranties are generally subject to an indemnification agreement from the signature guarantor, which may limit the amount and type of risks the signature guarantor will be liable for if the signature is determined not to be genuine.[37]

The electronic signature process that uses remote signing (transaction completed at the customer's home or business without a witness and without a manually created handwritten signature) does not include notaries, witnesses, unique manual handwriting, or signature guarantors. This process leaves the party enforcing the signature only with the initial presumption: a signature is genuine if provided on copies of a writing also signed by the adverse party, unless that adverse party denies the genuineness of his or her alleged signature in a verified pleading. If the adverse party denies the genuineness of the signature, the burden of proving its validity shifts back to the proponent of the signed writing; requiring the court to review the facts of the transaction to determine if, by a preponderance of the evidence, the signature is genuine.

V. ELECTRONIC SIGNATURE ATTRIBUTION

Farmer-customers who provide their electronic signatures on contracts do not always have witnesses present. Much of the electronic signature case law considers factual issues around intentions of the parties and authentication when the contracting parties are rarely face-to-face.

---

[34] *Id.*

[35] *See* U.C.C. § 8-306 (2014).

[36] *Id.* at § 8-306(h).

[37] *See Signature Guarantee Medallion Bond*, MERCER, http://www.brokerdealercoverage.com/ProductsAvailable/SignatureSignatureGuaranteeMeda.aspx (last visited Mar. 30, 2017).

As defined by the UETA, an electronic signature is 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."[38] The intent to sign can be an important issue in litigation.[39] Section 9 of the UETA establishes that "[a]n electronic record or electronic signature is attributable to a person if it was the act of the person."[40] Section 9 goes on to say that an "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."[41]

Courts evaluate the burden of proof when they consider signature attribution. A California federal court recently decided a case where the plaintiff, to whom the electronic signature was attributed, did not deny that an electronic contract belonged to him.[42] In that case, a declaration from the defendant that concluded the electronic signature was attributable to the plaintiff satisfied the defendant's attribution burden of proof.[43] Generally, when parties contest attribution, the inquiry frequently turns to the electronic security measures in place for tracing a signature back to the proper person.[44]

Two cases—one occurring in insurance and the other in retail—illustrate burdens of proof for contested electronic signatures.[45] A Michigan case, *Zulkiewski v. Am. Gen. Life Ins. Co.*, provides a good example of the security measures courts may consider when a party attempts to establish attribution.[46] There,

---

[38] *See* FLA. STAT. ANN. § 668.50(2)(h) (LexisNexis 2014).

[39] *See* J.B.B. Inv. Partners, Ltd. v. Fair, 182 Cal. Rptr. 3d 154, 164-5 (Cal. App. 1st Dist. 2014).

[40] UNIF. ELECTRONIC TRANSACTION ACT § 9 (1999).

[41] *Id.*

[42] Nanavati v. Adecco USA, Inc., 99 F. Supp. 3d 1072, 1074-5 (N.D. Cal. 2015).

[43] *Id.* at 1076 (distinguishing case facts from where the Plaintiff argued that the signature attributed to him was in fact not his. In Ruiz, the court held that the defendant's conclusory statement that the plaintiff signed electronically was not sufficient to prove attribution (citing Ruiz v. Moss Bros. Auto Group, Inc., 181 Cal.Rptr.3d 781, 840 (Cal. App. 4th Dist. 2014))).

[44] *See generally* Ruiz v. Moss Bros. Auto Group, Inc., 181 Cal.Rptr.3d 781, 840 (2014).

[45] *See* Zulkiewski v. Am. Gen. Life Ins. Co., No. 299025, 2012 WL 2126068, at *3 (Mich. App. June 12, 2012); Kerr v. Dillard Store Services, Inc., No. 07–2604–KHV, 2009 WL 385863, at *4-5 (D. Kan. Feb. 17, 2009).

the defendant-insurance company successfully satisfied its attribution burden by presenting evidence of how it not only was electronically provided the decedent's personal information (e.g., insurance policy number, social security number, mother's maiden name, and email address), "but also of email and regular mail notifications after the initial establishment of the e-Service account and subsequent beneficiary change."[47]

Alternatively, a Kansas federal court case, *Kerr v. Dillard Store Services, Inc.*,[48] provides an example of a party that failed to satisfy its attribution burden on security measures. There, the court noted the defendant-retailer's less-than-adequate procedures for maintaining secure intranet passwords, restricting access to arbitration agreements, determining whether electronic signatures were genuine as well as who accessed individual emails.[49] The court went on to rule that the defendant failed to prove by a preponderance of the evidence that the plaintiff executed the electronic agreement at issue.[50]

This section on statutory and case law presents two takeaways for lenders who present e-contracts to farmer customers without witnesses to the customer signature. First, lenders will want to draft language that makes it clear to customers that their signature represents their intent to contract.[51] Second, lenders will want to have system security features to show, by a preponderance of the evidence, attribution—that the person to whom the electronic signature is ascribed is the person who actually signed the agreement.[52]

---

[46] *See generally id.;* Stephen Mason, *Case Commentary: A Curious Case of Electronic Evidence (and Perhaps an Electronic Signature*), 12 AVE MARIA L. REV. 103, 103 (2014).

[47] *Zulkiewski*, 2012 WL 2126068, at *4.

[48] *See Kerr*, 2009 WL 385863, at *5.

[49] *Id.*

[50] *Id.*

[51] *See* Czapski, Michelle Thurber & Matthew R. Rechtien, *Who Pressed "Enter," Anyway? Enforcing Contracts in an Electronic World*, 54 No. 10 DRI For Def. 54 (2012).

[52] *Id.*

VI. PARTIES TO A CONTRACT: BURDENS OF PROOF

When discussing the burden of proof in contract cases, the Corpus Juris Secundum states the following:

> [T]he plaintiff has the burden to show the execution of the contract. "If the execution of the written contract is properly placed at issue, the burden of proof is on the party who asserts it." If the contract is expressly admitted, or its existence is not put in issue, the party alleging it is relieved of the burden of proving its execution.[53]

Once the proponent of contract validity has put forth admissible evidence, establishing that the contract was signed by the opponent, the burden shifts to the opponent; a mere assertion by the opponent that he or she did not sign the contract is, without supporting evidence, not sufficient to refute a finding that his or her signature was authentic.[54]

Evidence supporting contract validity is not limited to proof of the signing of the contract. Rather, acts performed by the opponent of the contract, that are consistent with its terms, may ratify the contract.[55] To allow a party to benefit from portions of the contract while allowing it to disavow others would be inequitable.[56] Accordingly, evidence of the opponent's contract performance may be admissible to show that the court should infer that the contract was signed by the opponent.[57]

A process for electronic commerce sets forth the steps in a business transaction: the customer purchase, customer signature, and completed sale. Courts examine the electronic transaction process—particularly the security safeguards in place for

---

[53] CONTRACT FROM VOLUME THIRTEEN CORPUS JURIS 758 (William Mack, LL.D. et al. eds., 1917).

[54] Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *3 (E.D. Mo. Mar. 6, 2009).

[55] Carter v. TD Ameritrade Holding Corp., 218 N.C. App. 222, 229 (N.C. Ct. App. 2012).

[56] *See* Fishman v. Gateway Inc., No 1 CA-CV 08-0125, 2009 WL 532558 , at 1 (Ariz. Ct. App. Mar. 3, 2009); *see also* Via Viente Taiwan L.P. v. United Parcel Serv., No. 4:08-CV-301, 2009 WL 398729, at *2 (E.D. Tex. Feb. 17, 2009).

[57] *See* In re Estate of Shama, 65 N.W.2d 360 (Iowa 1954).

signature attribution—as part of their analysis. The quintessential electronic transaction where benefits, and all facts and circumstances related to such benefits, are accepted by contract are general-purpose credit card transactions.

General-purpose credit card transactions minimize the risk of fraud for the lender by requiring merchants to compare unique characteristics of the customer's identity (appearance and handwriting) with the customer's card. Moreover, merchants may be liable to the processor or lender if they fail to meet this requirement and a card is used by someone other than the named cardholder.[58] This type of electronic transaction also minimizes the risk of repudiation (i.e., denial of assent to contract) by demanding, and sometimes recording, identification information relating to the transaction; this includes not only the use of government issued photo IDs to verify a customer's identity, but also the retention of unique signatures and records of the goods or services being provided to the customer. Again, the merchant may be held liable for the transaction if the customer successfully establishes a repudiation claim.[59]

A similar transaction is the DocuSign electronic signature process. This type of transaction was described by a federal district court in *Newton v. American Debt Services, Inc.*[60] In *Newton*, a customer contacted a merchant about purchasing services they advertised online. In response to the customer inquiring as to whether financing was available, the merchant referred him to a website application of a potential lender. Then, the customer and merchant engaged in a DocuSign electronic signature process, which generally requires the following:

1. The customer completes an application, which requires him or her to provide both public (e.g., address) and private information (e.g., cell phone and Social Security number).

---

[58] *Platform Payments 101*, WEPAY DEVELOPER 1, 16-17, https://www.wepay.com/files/payments-101.pdf.

[59] *See generally* U.S. v. Maze, 94 S. Ct. 645 (1974).

[60] Newton v. Am. Debt Servs., 854 F. Supp. 2d 712 (N.D. Cal. 2012).

2. The lender uses the information provided by the customer in the application, as well as other information (e.g., credit bureau reports), to make a credit decision. That credit decision includes ID theft safeguards that work to "red flag" and identify fraudulent applications submitted by parties posing as the customer.

3. The lender communicates the resulting credit approval status to the merchant and the customer.

4. If approved, the merchant prepares an electronic Purchase Order and the electronic credit documents.

5. The merchant sends the electronic documents to the customer using the DocuSign process. This email is an initial verification that the email address matches the email address on the application – something the customer has.

6. The customer receives a verification email sent to the address on the previously submitted application.

7. The customer opens the email and uses a link in that email message to access the DocuSign website.

8. The customer is given specific code numbers in that email message and the customer can then select the "Sign Now" box.

9. The customer may be called on the phone number provided in the application and asked to confirm that they want to sign electronically and provide those specific code numbers. This phone call is both an additional verification that the phone number matches the number on the application and a recording of a voiceprint.

10. A data base is accessed to create a series of multiple choice "out of wallet" (information that cannot be easily guessed or obtained from an internet search or a stolen wallet) questions to be presented to the customer that are used to ensure that the applicant is who they say they are. Typically, authentication is done through out-of-wallet questions drawn from credit reports and public records. The lender, working with the service provider, will configure the number of questions the applicant must answer and the score that must be achieved in order to authenticate the customer. The questions may include a "red herring" question which the customer will recognize as nonsensical. This knowledge based authentication uses something the customer knows.

11. The customer is presented with those questions.

12. The customer selects an answer for each question.

13. The customer's answers (something the customer knows) are used to further verify the customer's identity. If the customer cannot be positively verified, the process is ended.

14. Upon positive verification, the customer is then shown a dialogue box, explaining the terms of the electronic records and signatures process, where he is prompted to confirm he understands the terms by clicking on the consent and "Review Document" boxes.

15. The customer can then review all of the documents online.

16. The customer can then select a writing script to be applied to their name as the signature or use a mouse to create their signature.

17. The customer then applies that signature to all locations in the documents where it is required.

18. The customer then clicks "Confirm signing" which completes the customer electronic signing process and causes the electronic documents to be forwarded back to the merchant for any required merchant signatures.

19. The merchant signs the documents electronically, submits them to the lender, then the lender approves the credit transaction and sends the credit proceeds to the merchant.

20. The customer sends any required down payment amount to the merchant and the merchant then has the purchased goods or services delivered to the customer.

This DocuSign electronic signature process minimizes the risk of fraud for lenders by allowing them to combine the unique characteristics of a customer's identity (e.g., voiceprint), knowledge (e.g., "out-of-wallet" authentication questions), and contact information (e.g., email address) to verify that customer's identity.[61] Moreover, the process also decreases the risk of repudiation by providing the process description, retaining relatively unique voiceprint and knowledge based authentication answers, and recording the goods or services being provided to the customer.[62] Finally, both general-purpose credit card transactions and DocuSign electronic signatures create a nearly irrebuttable presumption that the customer agreed to the terms of the electronic contract; thus, a customer's mere denial of agreeing to the terms present in the electronic contract, without proof, will result in a valid contract.[63]

---

[61] *Id.*

[62] *See Are Electronic Signatures Legal?* DOCUSIGN (Apr. 12, 2017, 9:29 PM), https://www.docusign.com/learn/electronic-signature-legality; *see also* 15 USCS § 7001 (Lexis through Pub. L. 115-51).

[63] *See also* Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *1 (E.D. Mo. Mar. 6, 2009). Using a similar process and noting: "[w]hile new commerce on

VII. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL GUIDANCE ON ELECTRONIC SIGNATURES

The Federal Financial Institutions Examination Council ("FFIEC") is the joint federal banking agency that issues guidelines applicable to all US banks.[64] Many states also recommend compliance with those guidelines. The FFIEC issued guidance titled "Authentication in an Internet Banking Environment" ("Guidance") for those who are engaged in electronic commerce.[65]

The Guidance noted that, with the advent of technology and increasing use of the internet, banking transactions are often conducted online without any face-to-face interaction between bankers and customers.[66] These online transactions, due to vulnerabilities associated with internet banking systems, have become prone to risk of cyber-attacks in the form of identity theft, fraud, phishing, pharming,[67] malware,[68] and unauthorized access to accounts. Doing business with unauthorized or incorrectly identified persons in an internet banking environment thus can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

To counter this threat, the FFIEC issued the Guidance to encourage confidence among bankers and customers that the parties they engage with in electronic transactions are, in fact,

---

the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree." RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 23 (John A. Rothchild, eds., 2016). *See also* 2 Richard A. Lord, Williston on Contracts § 6:9 (4th ed. 1991) ("The acceptance of the benefit of services may well be held to imply a promise to pay for them if at the time of acceptance, the offeree has a reasonable opportunity to reject the service and knows or has reason to know that compensation is expected.").

[64] *About the FFIEC*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL (Aug. 3, 2016) https://www.ffiec.gov/about.htm.

[65] *See Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 1 (2005), https://www.ffiec.gov/pdf/authentication_guidance.pdf.

[66] *Id.* at 4.

[67] *Id.* at 4, n. 7.

[68] *Id.* at 4, n. 8.

who they say they are. The FFIEC's Guidance was intended to aid financial institutions in "evaluating and implementing authentication systems and practices whether they [were] provided internally or by a service provider."[69] The Guidance provides that "financial institutions should periodically ... [a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information."[70]

The Guidance describes the authentication processes as including three basic factors: (1) something the user knows (e.g., password, personal identification number); (2) something the user has (e.g., ATM card, smart card); and (3) something the user is (e.g., biometric characteristic, such as a fingerprint).[71] The Guidance also recommends more than one of those factors be used:

> Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out-of-band" controls for risk mitigation.[72]

The Guidance further states that single-factor authentication is particularly inadequate for higher risk transactions:

---

[69] *Id.* at 1.
[70] *Id.* at 2.
[71] *Id.* at 7.
[72] *Id.* at 3.

> The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. . . . Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.[73]

The layered approach is where one authentication factor is repeatedly used two or more times, such as requiring both a password and a personal identification number.[74]

There are other key points of the FFIEC Guidance that should be part of any electronic signature process:

> *Risk Assessment* – Financial institutions should perform periodic risk assessments of their internet banking systems.[75] The risk should be evaluated in light of the: (1) type of customer (e.g., retail or commercial); (2) customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); (3) sensitivity of customer information being communicated to both institution and customer; (4) ease of using communication method; and (5) volume of transactions.[76] The risk assessment process should: (1) identify all transactions and levels of access associated with internet-based customer products and services; (2) identify and assess risk mitigation techniques, including authentication methodologies, employed for each

---

[73] *Id.* at 1-4.

[74] *Supplement to Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL (2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf.

[75] *Authentication*, *supra* note 67 at 3.

[76] *Id.* at 3.

transaction type and level of access; and (3) include ability to gauge effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.[77]

Account Origination and New Customer Verification – Consistent with the United States PATRIOT Act, each financial institution must develop and implement an appropriate Customer Identification Program ("CIP") given its size, location and type of business.[78] The CIP must be written and incorporated into the financial institution's Bank Secrecy Act/Anti-Money Laundering program, and approved by the financial institution's board of directors.[79] The CIP must include risk-based procedures to verify the identities of customers (generally, persons opening new accounts).[80] Procedures in the program should describe how the financial institution will verify the identity of customer using documents, non-documentary methods, or a combination of both.[81] The procedures should reflect the institution's account opening processes, whether face-to-face or remotely, as part of the institution's e-banking services.[82]

---

[77] *Id.* at 4.

[78] *Customer Identification Program*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_011.htm (last visited Mar. 16, 2017).

[79] *Id.*

[80] *Id.*; *see also* Comptroller of the Currency Administrator of National Banks, *OCC Advisory Letter: Identity Theft and Pretext Calling*, OCC.GOV 5 (Apr. 30, 2001), https://www.occ.gov/static/news-issuances/memos-advisory-letters/2001/advisory-letter-2001-4.pdf (verification may be achieved in three ways (i) Positive Verification i.e. information provided by applicant matches information available from trusted third party sources; (ii) Logical Verification i.e. information provided is logically consistent (e.g. do telephone area code, ZIP code and street address match); and (iii) Negative Verification i.e. information provided has not previously been associated with fraudulent activity.)

[81] *Authenticating E-Banking Customers*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/authenticating-e-banking-customers.aspx?prev=1 (last visited Apr. 10, 2017) [https://perma.cc/Y9K9-VJK8].

[82] *Id.*

Monitoring and Reporting – Financial institutions should monitor unauthorized access to computer systems as well as customer accounts and report suspicious activities to appropriate regulatory and law enforcement agencies.[83]

Customer Awareness – Financial institutions should implement a customer awareness program and periodically evaluate its effectiveness.[84] The programs implemented by financial institutions should, at a minimum, include:

1. explanations of the circumstances and means by which financial institutions may contact their customers on an unsolicited basis to request their electronic banking credentials;

2. suggestions that commercial online banking customers perform related risk assessments and control evaluations periodically;

3. listing of (I) alternative risk control mechanisms customers may implement to mitigate risk; or (II) available resources where such information can be found; and

4. listing of institutional contacts for customers' discretionary use if they notice suspicious account activity or experience

---

[83] *Authentication*, *supra* note 67, at 5.

[84] *Id.* at 5-6 ("Methods to evaluate a program's effectiveness include tracking (i) number of customers who report fraudulent attempts to obtain their authentication credentials (e.g. ID/password); (ii) number of clicks on information security links on websites; (iii) number of statement stuffers or other direct mail communications; and (iv) dollar amount of losses relating to identity theft."); *see also Supplement*, *supra* note 85, at 7-8.

> customer information security-related events.[85]

VIII. ELECTRONIC CONTRACT PROVISIONS OF THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL INFORMATION TECHNOLOGY EXAMINATION HANDBOOK

Wide use of the Internet and technology evolution has transformed the way financial institutions deliver services. Financial institutions are now allowing customers to conduct a range of financial transactions (e.g., opening accounts, balance inquiries, and fund transfers) through their websites, which were previously unheard of. Though there are several benefits to using e-contracts for both banks and customers, many inherent risks remain.

To overcome these risks, the FFIEC developed The Information Technology Examination Handbook ("Handbook") to provide guidance to financial institutions on identifying and controlling risks associated with e-contracting.[86]

In summary, the Handbook provided the following information:

> *Systems* – Systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including internet, should be selected based on: (1) strategic objectives for E-Banking; (2) scope, scale and complexity of equipment, systems and activities; (3) technology expertise; and (4) security and internal control requirements.[87]

---

[85] *Supplement*, *supra* note 85, at 7-8.

[86] *IT Examination HandBook InfoBase*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/ (last visited Mar. 16, 2017) [https://perma.cc/ZXZ6-TKWL].

[87] *E-Banking Components*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/introduction/e-banking-components.aspx (last visited Mar. 16, 2017) [https://perma.cc/H2MU-9J4E].

> *Risks* – Risks associated with e-contracts include (1) Transaction/Operations Risk (arising from fraud, processing errors, system disruptions or other unanticipated events resulting in an inability to deliver products/services);[88] (2) Credit Risk (arising from aspects like (a) verifying customer's identity for on-line credit applications and executing enforceable contract; (b) valuing collateral and perfecting liens over wide geographic area; and (c) collecting loans from individuals over wide geographic area etc.);[89] (3) Compliance/Legal Risk (arising from establishment of legally binding e-contracts and uncertainty over laws and jurisdictions);[90] (4) Strategic Risk (arising from poor planning and investment decisions);[91] and (5) Reputation Risk (arising from unauthorized activity, disclosure/theft of confidential customer information etc.).[92]

These risks can be managed with appropriate oversight, including cost-benefit analysis, risk assessment, and due diligence processes for evaluating e-contracting activities.[93] The

---

[88] *Transaction/Operations Risk*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/transactionoperations-risk.aspx (last visited Mar. 16, 2017) [https://perma.cc/SV8M-6TV6].

[89] *Credit Risk*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/credit-risk.aspx (last visited Mar. 16, 2017) [https://perma.cc/YMT2-A7KX].

[90] *Compliance/Legal Risk*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL., http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/compliancelegal-risk.aspx (last visited Mar. 16, 2017) [https://perma.cc/EGJ7-MZCA].

[91] *Strategic Risk*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/strategic-risk.aspx (last viewed Mar. 16, 2017) [https://perma.cc/4AZ2-RHDN].

[92] *Reputation Risk*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/e-banking-risks/reputation-risk.aspx (last viewed Mar. 16, 2017) [https://perma.cc/ER99-UYFS].

[93] *Cost-Benefit Analysis and Risk Assessment*, FED. FIN. INST. EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/board-and-management-oversight/cost-benefit-analysis-and-risk-assessment.aspx (last viewed Mar. 16, 2017) [https://perma.cc/A4VN-K7WZ].

electronic contracting strategy should be periodically monitored and audited.[94]

> *Managing Outsourcing Relationships* – There also must be effective oversight of third-party vendors by ensuring: (1) effective due diligence in selection of new service providers in terms of financial condition, experience, expertise, technological compatibility, and customer satisfaction; (2) that written contracts contain provisions relating to privacy/security of data, right to audit security/controls, monitoring service quality, limiting financial institutions liability for acts of service provider and termination of contract; and (3) vendor's service quality, security controls and stability are monitored.[95]
>
> *Information Security Program* – Financial institutions should (1) ensure compliance with "Guidelines Establishing Standards for Safeguarding Customer Information" issued pursuant to Gramm-Leach-Bliley Act, 1999; (2) ensure the institution has the appropriate security expertise for its e-banking platform; and (3) implement security controls sufficient to manage unique security risks confronting financial institutions.[96]
>
> *Internal Controls* – Financial institutions should consider the following controls (a) segregation of duties to minimize employee fraud; (b) dual-control procedures for sensitive electronic contracting

---

[94] *Managing Outsourcing Relationships*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/managing-outsourcing-relationships.aspx (last viewed Mar. 16, 2017) [https://perma.cc/KR7V-GMFX].

[95] *Id.*

[96] *Information Security Program*, FED. FIN. INSTITUTIONS EXAMINATION COUNCI., http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program.aspx (last viewed Mar. 16, 2017) [https://perma.cc/8UKK-N3RS].

> activities like access to encryption key; (c) fraud detection and review of suspicious activities, like multiple new accounts; (d) periodic monitoring of internet to detect websites with similar names, possibly established for fraudulent purposes; (e) error checks and customer guidance to prevent unintentional errors; (f) alternate channel confirmations to ensure account activity is authorized; and (g) business disruption avoidance strategies and recovery plans.[97]
>
> *Legal and Compliance Issues* – Financial institutions should also: (1) identify official names of financial institutions providing electronic contracting services; (2) disclose customer privacy and security policies on their websites; and (3) ensure that advertisements, notices, and disclosures are in compliance with applicable statutes and regulations, including the E-Sign Act.[98]

Financial institutions should adapt the processes examined above to address and mitigate risks associated with e-contracting activities.

IX. ENFORCEABILITY OF E-SIGNATURE AND AUTHENTICATION PROCESS WITH PRIOR PAPER PEN AND INK SIGNED AGREEMENT

Traditional paper contracts can still have a place in electronic commerce. Some financial institutions use the process of first entering into a paper agreement with a customer via an

---

[97] *See Internal Controls*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/administrative-controls/internal-controls.aspx (last viewed Mar. 16, 2017) [https://perma.cc/JA9J-YYZA].

[98] *See Legal and Compliance Issues*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/legal-and-compliance-issues.aspx (last viewed Mar. 16, 2017) [https://perma.cc/27HX-MXTJ].

in-person signing. A key provision in these paper agreements is how the financial institution and the customer will acknowledge the customer's electronic signature. In the paper agreement, the customer will stipulate that, for future transactions, an approval that the financial institution receives from any person using a designated email address, phone number, code, or some other method that the customer chooses, will be the customer's legal signature when making an offer, accepting an offer, or otherwise creating a contract. This section includes selected cases on the enforceability of this type of paper and ink agreement and the electronic legal signatures it creates.

A paper agreement with a customer as described above is supported by general contract law principles. This includes the mutual assent of the parties which requires an offer, acceptance, and consideration.[99] Thus, a contract will be created when an offer is accepted according to the offer's prescribed time, place, or manner for valuable consideration.[100] Courts also generally presume a written and signed agreement is supported by consideration.[101]

This is also consistent with the general freedom of contract. Iowa courts have recognized the "weighty societal interest in the freedom of contract," pursuant to which private parties are permitted to enter into contracts that govern their personal interactions.[102] The state's courts enforce contracts because they are a product of the free will of the parties who, within limits, are permitted to define their own obligations.[103] Iowa courts bind parties to agreements into which they freely and knowingly enter.[104]

A prior agreement between the parties is also consistent with the Iowa Uniform Commercial Code's requirements for

---

[99] *See* Margeson v. Artis, 776 N.W.2d 652, 655 (Iowa 2009). It also includes an offer to contract. Magnussen Agency v. Public Entity Nat'l Co.-Midwest, 560 N.W.2d 20, 26 (Iowa 1997); and includes acceptance. Heartland Express, Inc. v. Terry, 631 N.W.2d 260, 270 (Iowa 2001).

[100] *See* Flanagan v. Consolidated Nutrition, L.C., 627 N.W.2d 573, 578 (Iowa Ct. App. 2001); *see also* Hinshaw v. Ligon Indus., L.L.C., 551 F. Supp. 2d 798, 813 (N.D. Iowa 2008); RESTATEMENT (SECOND) OF CONTRACTS, §§ 30, 50 (1981).

[101] *Margeson*, 776 N.W.2d at 656.

[102] Walker v. Gribble, 689 N.W.2d 104, 111 (Iowa 2004).

[103] *See* Iowa v. Baldon, 829 N.W.2d 785, 792 (Iowa 2013).

[104] Breitbach v. Christenson, 541 N.W.2d 840, 845 (Iowa 2000).

"authenticating" security agreements. That is, the Uniform Commercial Code requires parties to sign, execute, or otherwise adopt a sound, symbol, or process with the present intent of the authenticating person to identify the person and adopt or accept a record.[105] A "record" is "information . . . inscribed on a tangible medium or which stored in an electronic or other medium and is retrievable in perceivable form."[106]

Finally, such an agreement is also supported by the general rule that transaction information purporting to establish or terminate a contract, such as phone call statements, are admissible as evidence of a contract so long as it is supported by circumstantial evidence.[107] An electronic transaction purporting to create a contract that includes the completing of the specific pre-agreed process would constitute significant circumstantial evidence.[108]

This process of entering into a witnessed paper agreement with a customer in which the customer will agree that, in the future, an approval received by the financial institution, using a specific process, can create a new contract has its limitations. It cannot be used for persons who are not available for initial face-to-face contact. Also, each new contract created using that process must follow the exact agreed upon process.[109] The ability of the parties to agree on what constitutes an approved authentication was upheld in *Choice Escrow*. In that case, the court concluded that an approved wire transfer occurred where a bank and its customer agreed on an authentication process and then used that process.[110]

---

[105] IOWA CODE § 554.9102(1)(g) (2013).

[106] IOWA CODE § 554.9102(1)(br) (2013).

[107] *See* Texas Candy & Nut Co. v. Horton, 235 S.W.2d 518 (Tex. App., 1950); Morris v. Texas, 460 S.W.3d 190 (Tex. App. 2015); Passovoy v. Nordstrom, Inc., 758 P.2d 524 (Wash. Ct. App.1988); Cox v. Cline, 126 N.W. 330 (Iowa. 1915); Cavanagh v. Ohio Farmers Ins. Co., 509 P.2d 1075 (Ariz. Ct. App. 1973); Campbell v. Wilson, 117 N.W.2d 620 (Wis. 1962).

[108] *See* SN4, LLC, v. Anchor Bank, FSB, 848 N.W.2d 559, 566-67 (Minn. Ct. App. 2014).

[109] *Id.* at 567.

[110] Choice Escrow & Land Title, LLC v. BancorpSouth Bank, 754 F.3d 611, 617 (8th Cir. 2014).

X. AUTHENTICATION METHODS BEYOND PUBLIC RECORD KNOWLEDGE-BASED QUESTIONS

Contracting parties have a variety of options for authenticating a remotely-signed electronic signature. However, information systems professionals often stop short of saying that any one option guarantees perfect authentication.[111] Instead, these professionals and other e-commerce contributors weigh the costs and benefits, along with the customer experience, for each available option.[112] The following section provides a survey of options for authenticating a remote signer of e-contracts.

The password is unique to the signer and can be a way to link the electronic signature back to the signer for authentication purposes.[113] Although common, passwords have two drawbacks: (1) signers can forget their password; and (2) signers (in an attempt to avoid forgetting their password) might devise a simple password that others can easily guess and use to gain signer access.[114] These drawbacks lead some information systems professionals to predict that other authentication options might supplant passwords as more effective tools.[115]

As an alternative to passwords, signers might use codes, tokens, or smartcards to gain access to electronic documents and authenticate their signatures.[116] These options, grouped together, are "something the user has" to authenticate signatures.[117] To access the document to be electronically signed, signers will type in an assigned code or insert an assigned token or smartcard to

---

[111] Aimee Rhodes, *10 Chief Information Security Officers (CISOs) Say Passwords Are Failing and Must Be Augmented or Supplanted*, PRNEWSWIRE (Jan. 28, 2016), http://www.prnewswire.com/news-releases/10-chief-information-security-officers-cisos-say-passwords-are-failing-and-must-be-augmented-or-supplanted-300211282.html [https://perma.cc/WP5R-7JW4].

[112] *See id.*

[113] *Authenticating E-Banking Customers*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/information-security-program/authenticating-e-banking-customers.aspx (last visited Mar. 16, 2017) [https://perma.cc/8W6U-ZHDR].

[114] *Id.*

[115] Rhodes, *supra* note 122.

[116] *Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/media/28217/ncu-05-cu-18-encl-1.pdf (last visited Mar. 16, 2017) [https://perma.cc/FN42-VGUA].

[117] *Id.*

associate the signers with their signatures.[118] Assigned codes, tokens, and smartcards can be improvements over signer-created passwords because hackers are less likely to guess the passcode sequencing.[119] But these "something-the-user-has" options still present risks when signers misplace these identification devices (e.g., leaving them to be found by others who can gain access).[120]

Parties who wish to avoid the drawbacks of "something-the-user-has" options (e.g. forgotten codes, stolen codes, and lost codes) might explore biometric authentication codes. These codes use the personal attributes of the signer such as fingerprints and voice to electronically identify the signer.[121] If passwords, codes, tokens, and smartcards are "something the user has" to authenticate, then biometric qualities represent "something the user is."[122]

Biometrics for electronic signature authentication are relatively new with a few options available for parties.[123] One biometric option is using a signature pad that captures the signer's fingerprint for signature authentication.[124] Another biometric option measures the uniqueness of one's own stored signature as a way to authenticate.[125] These "something-the-user-is" options offer more certainty when authenticating an electronic signature because it is difficult to copy or misappropriate unique human qualities.[126] Implementation costs and the invasiveness signers might experience when providing their fingerprints or iris scans for authentication are drawbacks for biometric options.[127]

---

[118] *Id.* at 7.

[119] *See id.* at 3.

[120] *Id.* at 10.

[121] *Id.* at 9-10.

[122] *Id.* at 3.

[123] R.R. Jueneman & R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS 1 (1998), mcwg.org/mcg-mirror/mirrors/digsig.pdf [https://perma.cc/V7X9-FMAF].

[124] BIOMETRICS INST., http://www.biometricsinstitute.org/pages/types-of-biometrics.html (last viewed Apr. 4, 2017) [https://perma.cc/4J3H-6C6A]; *Biometric ID Pads*, TOPAZ SYSTEMS INC., http://www.topazsystems.com/idpads.html (last visited Apr. 4, 2017) [https://perma.cc/4F55-D8SJ].

[125] *See* Jueneman, *supra* note 134, at 2.

[126] See *Authentication in an Electronic Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 10 (Aug. 8, 2001), https://www.ffiec.gov/pdf/pr080801.pdf [https://perma.cc/AKK3-N6GA].

[127] *Id.* (users may associate fingerprinting with law enforcement).

Security questions are another option for contracting parties.[128] For authentication with security questions, signers answer questions asked of them regarding personal information that only the signer is likely to know.[129] The electronic document platform stores the signer's answers.[130] Such questions might include previous residence addresses, the maiden name of the signer's mother, and the signer's favorite book.[131] Signers must answer several security questions correctly in order to access the electronic document.[132] These security questions offer a similar positive as "something-the-user-is" options; namely, it requires security answers that are unique to the signer and consequently difficult for others to misappropriate.[133] Potential drawbacks include: (1) the signers' forgetfulness in remembering how they previously answered the security question; and (2) the difficulty in choosing an adequate number of questions to set the security bar appropriately high.[134]

XI. CONCLUSION

Our recommendations for authentication of remote electronic signatures, as well as a comparison of evidentiary standards between goods and services financing and fund transfers, are based on existing electronic signature law and industry and regulator guidance. A robust electronic signature authentication process cannot be static. It must evolve with changes in technology, industry wide best practices, and tactics used by the bad actors that are trying to fool commonly used authentication processes. Like paper and ink contracts, the signer authentication will not be 100 percent verifiable. Accordingly, the goal should be to manage risks by including

---

[128] Richard Spillenkothen, *Interagency Guidance on Authentication in an Internet Banking Environment*, BOARD GOVERNORS FED. RES. SYS. 7 (Oct. 13, 2005), http://ithandbook.ffiec.gov/media/resources/3371/frb-sr-05-19.pdf [https://perma.cc/99C2-YBQ6].

[129] *Id.* at 13.

[130] *Id.* at 8.

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

enough authentication and ratification factors in the signing transaction, and after the signing transaction, to create a significant presumption that the appropriate person electronically signed the contract. A multi-factor process for electronic signature authentication might include a combination of some of the following elements:

- Use of the email address provided by the customer (something the customer has);
- Use of the phone number provided by the customer (something the customer has);
- Use of a computer owned by the customer (something the customer has);
- Use of an IP address assigned to the customer (something the customer has);
- Capture of a customer voice print (something the customer is);
- Customer responses to "out of wallet" questions that it is unlikely anyone other than the customer could have answered within the time allowed for response (knowledge based authentication- something the customer knows);
- Records of delivery of the purchased goods or services to the customer (including state issued photo ID verification of a contract signer at the time of delivery) – contract ratification;
- Records of customer receipt of a confirmation email and no response (contract ratification);
- Records of the receipt of credit account payments by the customer (contract ratification); and/or

- Records of other customer behavior ratifying the contract, such as use of the provided goods or services (contract ratification).

The use of email confirmation immediately after the transaction may be an appropriate additional verification. This confirmation can serve as evidence of an agreement and as a fraud control method.

In addition to designing an authentication process with several factors in place, lenders may need to include a risk-based selection of authentication methods. With risk-based triggers, additional authentication would be required for higher dollar transactions and transactions that are anomalous for the customer. Risk-based selections can provide heightened awareness for a transaction above a certain pre-determined dollar threshold or for a large dollar amount that is out of character based on the customer-signer's purchase history.

For courts, a party's electronic signature authentication process goes to the heart of evidentiary burdens. The standard here is one of sufficiency: Does the evidence of authentication and ratification create such a presumption of contract validity that it cannot be overcome by whatever contrary evidence, if any, put forth by the customer?[135] Some authentication cases involving payment systems have also required that the process be commercially reasonable, but that is only because the section of the Uniform Commercial Code regarding funds transfers adds that requirement to any agreed upon security procedure.[136] In the goods and services financing area, the issue is evidentiary sufficiency, instead of commercial reasonableness.

Customer comfort with technology, the increasing distance between customers and suppliers, and ongoing process improvement within the agricultural industry all support

---

[135] *See* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 212-13 (1st Cir. 2012); *see also* U.C.C. § 4A-202(2) (2016).

[136] § 4A-202(2) (stating while fund transfers are not a focus of this article, the U.S. First Circuit Court of Appeals case of *Patco*, 684 F.3d 197, features a thorough analysis of the kinds of fact issues involved in fund transfer authentication); *see also* Melissa Waite, *In Search of the Right Balance: Patco Lays the Foundation for Analyzing the Commercial Reasonableness of Security Procedures Under UCC Article 4A*, 54 B.C. L. REV. E-SUPP. 217 (2013).

electronic signature as a lender solution. The one constant amongst the evolving electronic signature technologies, however, is electronic signature authentication. A well-developed, multi-factor signer authentication process is vital to ensure that there is balance between commercial efficiency and protection for the contracting parties.

SAMPLE CUSTOMER ELECTRONIC SIGNATURE ASSENT LANGUAGE

"I adopt this signature facsimile as my signature, used by DocuSign."[137]

SAMPLE AGREEMENT TO SIGN AND CONTRACT ELECTRONICALLY

CONSUMER DISCLOSURE

From time to time, ABC Company (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign, Inc. (DocuSign) electronic signing system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print

[137] S*ee* DOCUSIGN (Sept. 19, 2017, 9:00 AM), https://go.docusign.com/trial/sign-anywhere/?elqCampaignId=4481&utm_source=google&utm_medium=cpc&utm_campaign=branded_secondary&utm_term=docusigne&utm_content=domestic_US&gclid=CNqylMvGz8kCFZAAaQodlX8DOA.

documents we send to you through the DocuSign system during and immediately after signing session and, if you elect to create a DocuSign signer account, you may access them for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you may be charged a $1.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of a DocuSign envelope instead of signing it. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact ABC Company:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: ABCCustomerService@.com

To advise ABC Company of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at ABCCustomerService@.com and in the body of such request you must state: your previous email address and your new email address. We do not require any other information from you to change your email address.

To request paper copies from ABC Company

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to ABCCustomerService@.com and in the body of such request you must state your email address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with ABC Company

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your DocuSign session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to ABCCustomerService@.com and in the body of such request you must state your email, full name, US Postal Address, and telephone number. We do not need any other information from you to withdraw consent. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process.

Required hardware and software

Operating Systems:	Windows® 2000, Windows® XP, Windows Vista®; Mac OS® X
Browsers:	Final release versions of Internet Explorer® 6.0 or above (Windows only); Mozilla Firefox 2.0 or above (Windows and Mac); Safari™ 3.0 or above (Mac only)
PDF Reader:	Acrobat® or similar software may be required to view and print PDF files
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	Allow per session cookies

** These minimum requirements are subject to change. If these requirements change, you will be asked to re-accept the disclosure. Pre-release (e.g. beta) versions of operating systems and browsers are not supported.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to email this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify ABC Company as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by ABC Company during the course of my relationship with you.

Text Added to All U.S. ABC Company Installment Equipment Finance Contracts

You agree that this Contract is an electronic record executed by you using your electronic signature. You acknowledge and agree that, by executing this Contract with your electronic signature, you are signifying your intent to enter into this Contract and that this Contract be legally valid and enforceable in accordance with its terms to the same extent as if you had executed this Contract using your written signature. You agree that unless the authoritative electronic copy of this Contract ("Authoritative Copy") is converted to paper and marked as the original by us (the "Paper Contract"), the Authoritative Copy shall at all times reside in a document management system designated by us for the storage of authoritative copies of electronic records (the "DMS"), and shall be deemed held in the ordinary course of business. In the event the Authoritative Copy is converted to a Paper Contract, you acknowledge and agree that (1) your signing of this Contract also constitutes issuance and delivery of such Paper Contract, (2) your electronic signature associated with this Contract, when affixed to the Paper Contract, constitutes your legally valid and binding signature on the Paper Contract, and (3) your obligations will be evidenced by the Paper Contract alone after such conversion.