

IN THE SUPREME COURT OF TEXAS

No. 20-0290

AEROTEK, INC., PETITIONER,

v.

LERONE BOYD, MICHAEL MARSHALL, JIMMY ALLEN,
AND TROJUAN CORNETT, RESPONDENTS

ON PETITION FOR REVIEW FROM THE
COURT OF APPEALS FOR THE FIFTH DISTRICT OF TEXAS

Argued February 23, 2021

CHIEF JUSTICE HECHT delivered the opinion of the Court, in which JUSTICE GUZMAN, JUSTICE LEHRMANN, JUSTICE DEVINE, JUSTICE BLACKLOCK, JUSTICE BUSBY, JUSTICE BLAND, and JUSTICE HUDDLE joined.

JUSTICE BOYD filed a dissenting opinion.

Contracts are increasingly signed electronically, with an online click for every kind of transaction imaginable—from simple, everyday retail purchases to complex matters of great consequence. The utility of digital contracts depends heavily, of course, on their enforceability as a matter of law. The Texas Uniform Electronic Transactions Act (the Act)¹ states that “[a]n electronic record or electronic signature is attributable to a person [by] showing . . . the efficacy of any security procedure applied to determine the person to which the electronic record or electronic

¹ TEX. BUS. & COM. CODE ch. 322.

signature was attributable.”² The issues before us are how the efficacy of a security procedure is shown and, once it is, whether the alleged signatory’s simple denial that he signed the record is sufficient to prevent attribution of an electronic signature to him. We hold here that attribution was conclusively established and therefore reverse the judgment of the divided court of appeals.³

I

A

Aerotek hires employees globally by the hundreds of thousands to work as contractors for client companies. To keep hiring efficient, Aerotek worked with a software developer to build an online-only hiring application. Aerotek exclusively uses this computerized hiring application to guide employee candidates through the hiring process—a process sometimes referred to as “onboarding”. Aerotek’s hiring application automatically sends a welcome email to the email address the candidate has provided during the recruitment and initial interview process. The welcome email includes a unique hyperlink for the candidate to use to navigate to the hiring application’s online account-registration page. Once there, the candidate creates a unique user ID and password and selects security questions. To later log in to the hiring application, the candidate must enter this user ID, password, and security-question combination correctly. This login process takes place each time the candidate leaves and returns to the hiring application.

The computerized hiring application presents the candidate with employment information and various contracts to sign electronically. The first document requiring an electronic signature is an Electronic Disclosure Agreement (EDA). By signing the EDA, the candidate consents to “be

² *Id.* § 322.009(a).

³ ___ S.W.3d ___ (Tex. App.—Dallas Aug. 27, 2019).

bound” by Aerotek’s electronic hiring documents “as though . . . signed . . . in writing.” After the candidate signs the EDA, the application presents other documents to the candidate for completion and signature. These documents ask for personal information, such as addresses and emergency contacts. The application requires candidates to complete and electronically sign the documents in a particular order. After the candidate completes the initial documents, the application unlocks four additional documents, including a Mutual Arbitration Agreement (MAA). The candidate may electronically sign these documents in any order, but he must complete all four before the computerized application will allow him to continue and complete the hiring process.

As the candidate enters information and signatures on the documents, the hiring application tracks his progress. For nearly every action the candidate takes, the hiring application stores an electronic record in a database. For instance, each time a candidate electronically signs a document the hiring application stores a new electronic record that includes the candidate’s unique identifier, the type of document, and a timestamp showing the date and time the document was signed. Once the application records that information, Aerotek cannot change it.

A candidate who claims to lack the ability to use the computerized hiring application is invited to Aerotek’s office for assistance. But the candidate must still go through the hiring application step by step, providing the same information and signatures that would be required if he were not assisted.

B

Trojuan Cornett, Michael Marshall, and Lerone Boyd each completed Aerotek’s computerized hiring application on his own. Jimmy Allen completed his in Aerotek’s office with assistance from Sybil Harper, an administrative assistant. Their completed applications all include

an MAA, timestamped with their signature just a few minutes after they signed the EDA.⁴ Aerotek hired all four (the Employees) to work as contractors on a construction project for Aerotek's client, J.R. Butler, Inc. All four were terminated not long after starting work and sued Aerotek, Butler, and others for racial discrimination and retaliation.⁵

Aerotek moved to compel arbitration. It attached to its motion each Employee's timestamped EDA and MAA, along with database records showing the timestamp for every other action taken by each Employee in completing the hiring application. The Employees opposed the motion. Represented by the same lawyer, each submitted a sworn declaration acknowledging that he had completed the online hiring application but denying that he had ever seen, signed, or been presented with the MAA. In substance, the four declarations are word-for-word identical; Allen's differs only in its acknowledgment that he was assisted by Harper.⁶

⁴ From start to finish, the record shows that the Employees each took only a few minutes to complete the hiring application. For Cornett, timestamps show that he electronically signed the EDA on "11/15/16 11:29 PM" and the MAA on "11/15/16 11:56 PM". He submitted his application for review on "11/16/16 12:15 AM". For Marshall, timestamps show that he electronically signed the EDA on "11/17/16 6:31 PM" and the MAA on "11/17/16 6:42 PM". He submitted his application for review on "11/17/16 6:43 PM". For Boyd, timestamps show that he electronically signed the EDA on "11/22/16 10:32 AM" and the MAA on "11/22/16 11:02 AM". He submitted his application for review on "11/22/16 11:07 AM". And for Allen, timestamps show that he electronically signed the EDA on "3/14/17 4:22 PM" and the MAA on "3/14/17 4:31 PM". He submitted his application for review on "3/14/17 4:32 PM".

⁵ None of the other defendants are parties to this proceeding.

⁶ The other three Employees swore in their declarations that they were "required to review and agree to certain terms, conditions, policies and/or procedures" as part of the onboarding process. These they "reviewed . . . online and signed . . . electronically." However, they all denied ever having "seen", "reviewed," been "presented with", or "sign[ed] any document, electronically or otherwise, [agreeing to] arbitrate claims against Aerotek". Nor were they otherwise "told" about or asked to "consent" to the MAA. In sum, they swore that "no one from Aerotek . . . ever mentioned arbitration to [them] before this lawsuit was filed."

Allen swore similarly to the other Employees in his declaration. He, too, admitted that he "reviewed and agreed to" Aerotek's "terms, conditions, policies and/or procedures" online as part of his onboarding process. He, too, denied ever having "seen", "reviewed", "sign[ed]", been "told" about or "presented with", or otherwise "consented[]" to" any arbitration agreement. Unlike the other Employees, though, Allen swore that he "was not computer savvy", and so he "sat with" an Aerotek administrative assistant, Sybil Harper, who "went through and signed all [his] paperwork electronically".

The trial court conducted an evidentiary hearing on Aerotek’s motion to compel. Phaedra Marsh, a program manager who had worked for Aerotek for nearly 20 years, testified that while Aerotek personnel did not write the computer code themselves, she helped design and develop the application by defining how it would operate—specifications sometimes referred to as “business rules”.⁷ The software developer then reduced those business rules to computer-readable code. Marsh testified that although she was neither part of Aerotek’s IT department nor an IT expert, she did all the hiring application’s testing, managed its updates and enhancements, and directed the training that Aerotek provided internally. Marsh also performed an in-court demonstration on a laptop and external monitor to show how each step in the hiring-application process worked. Asked whether there was any possible way the Employees could have completed their applications without executing the MAA, Marsh answered: “Not with this process. It’s locked throughout . . . , so they have to complete everything in that section before they can get to the finalize-and-submit section. So everything has to be signed and completed before they get there.” Further, she added, “[w]e don’t have the ability to alter [forms] after they’re submitted” by a candidate. Marsh testified that the hiring-application process had not changed since the Employees used it. The only glitch she described in the use of the hiring application was when one of the four servers housing the data for the system went down, with the result that a candidate could not

⁷ See Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEXAS L. REV. 669, 707 (2010); see also Peter DiCola & David Touve, *Licensing in the Shadow of Copyright*, 17 STAN. TECH. L. REV. 397, 443 n.189 (2014) (“In software development, business logics are the parts of the underlying computer code that reflect rules about what data will be displayed and what data the user can enter.”); David Kiefer & Marc Lauritsen, *Recent Developments in Automating Legal Documents*, 52 SYRACUSE L. REV. 1091, 1093 (2002) (describing how “complex business logic rules” are used by law firms to automate their workflow); Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305, 1317 (2019) (describing how legal experts and computer programmers work together to define a computer application’s “formal rules” that enable it to complete a legal task, like filing taxes).

immediately respond to the welcome email's invitation to use the application.

Aerotek's only other witness was the administrative assistant that assisted Allen, Sybil Harper. She testified that while she assisted Allen in completing his application as shown by the computer record, she did not recall the event specifically. Harper testified that she uses a "very strict" and "very structured" process for assisting candidates with the hiring application. Over "a hundred times" she has sat "next to" candidates in "a designated computer lab" to personally assist them with completing the hiring application. She starts out by helping the candidate to retrieve Aerotek's welcome email from the candidate's personal email. Then she assists candidates, as needed, with using the welcome email to navigate to the hiring application and create their user name and password. From there, Harper assists the candidate with "start[ing] the on-boarding process." Harper ensures that "[e]verything is entered" and "signed electronically", including the "electronic disclosure", "biographical information", and other documents, such as the "arbitration agreement". Harper also testified that at "each step as [they] go through with the process" she gets renewed "consent" to continue. She also stated that she cannot "bypass" the hiring application's business rules and has never "electronically attached someone's signature to any document"—including an arbitration agreement—without the person's consent. "[E]verything has to be done in order," Harper explained, and "[b]y the end of it" she assists the candidate with finishing the application through "the finalize and submit process."

The Employees offered only their declarations as evidence, the parties having agreed that the court could consider the declarations as sworn testimony in open court.

The trial court denied Aerotek's motion to compel arbitration. A divided panel of the court of appeals affirmed. The majority rejected Aerotek's argument that it had conclusively established

the MAAs' validity. The majority concluded that Marsh had "insufficient capacity to establish the system was failsafe" since she was "not an IT expert".⁸ Her in-court demonstration of the hiring application, the majority said, showed merely "what happened in the system that day in court", not necessarily what the Employees had actually experienced.⁹ The majority reasoned that "Marsh never vouched for the [database] records' integrity, nor could she adequately explain the security measures Aerotek took."¹⁰ The majority noted that Aerotek "did not bring a witness from" the software developer that created the hiring application "to provide technical explanation and vouch for the system security."¹¹ In any event, the majority concluded, Marsh was an interested witness whose testimony the trial court was free to discount, especially if there were demeanor and credibility issues not apparent on the face of the record.¹² The Act did not influence its analysis, the majority reasoned, because it does not provide a "framework of appellate review".¹³ The majority also concluded that Harper's "total lack of specific memory as to her dealings with" Allen failed to conclusively establish that he had signed the MAA.¹⁴

The dissent took issue with the majority's analysis, arguing that it set "a standard that would make electronic contract formation practically impossible and write section 322.009 out of the

⁸ __ S.W.3d at __.

⁹ *Id.* at __ n.4.

¹⁰ *Id.* at __.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.* at __.

¹⁴ *Id.* at __.

law.”¹⁵ The court denied Aerotek’s motion for rehearing en banc over a dissent joined by four Justices.¹⁶

We granted Aerotek’s petition for review.

II

To compel arbitration, a party must prove that a valid arbitration agreement exists.¹⁷ For the MAAs to be valid, the Employees must have consented to them.¹⁸ The Employees argue only that they did not consent to the MAAs because the electronic signatures on the agreements are not theirs. They admit that they completed Aerotek’s online hiring application but deny that they were presented with the MAAs during that process. The trial court believed them.

We must defer to the trial court’s factual finding that the Employees did not sign the MAAs if that finding is “supported by evidence”.¹⁹ Aerotek contends that it conclusively established that the Employees signed the MAAs by proving that the security procedures for its hiring application would have made it impossible for the Employees to complete their applications without signing the MAAs during that process. “Evidence is conclusive only if reasonable people could not differ in their conclusions, a matter that depends on the facts of each case.”²⁰

For a paper document with a handwritten, wet-ink signature, the genuineness of the

¹⁵ *Id.* at __ (Bridges, J., dissenting).

¹⁶ 598 S.W.3d 373 (Tex. App.—Dallas 2020) (Schenck, J., dissenting from the denial of reh’g en banc).

¹⁷ *Henry v. Cash Biz, LP*, 551 S.W.3d 111, 115 (Tex. 2018) (citation omitted).

¹⁸ *USAA Tex. Lloyds Co. v. Menchaca*, 545 S.W.3d 479, 501 n.21 (Tex. 2018) (citations omitted).

¹⁹ *Henry*, 551 S.W.3d at 115 (“We review a trial court’s order denying a motion to compel arbitration for abuse of discretion. We defer to the trial court’s factual determinations if they are supported by evidence but review its legal determinations de novo.” (citing *In re Labatt Food Serv., L.P.*, 279 S.W.3d 640, 642–643 (Tex. 2009) (orig. proceeding))).

²⁰ *City of Keller v. Wilson*, 168 S.W.3d 802, 816 (Tex. 2005) (citation omitted).

signature can be proved by direct evidence—for example, testimony by an eyewitness, a witness familiar with the signatory’s handwriting, or an expert who has compared the signature against a genuine specimen.²¹ But these authentication methods may not be applicable to a purely electronic signature.²² While handwritten signatures are unique to an individual, electronic signatures sometimes involve nothing more than clicking a box online and recording the information in an electronic database.²³

Once parties to a transaction have “agreed to conduct [it] by electronic means”,²⁴ the Act provides a standard for attributing electronic signatures to them. Section 322.009(a) provides that an “electronic signature is attributable to a person if it was the act of the person.”²⁵ That “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.”²⁶ Section 322.002(13) defines a security procedure as any “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”, including “the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other

²¹ See TEX. R. EVID. 901.

²² We express no opinion on how to authenticate a handwritten signature created electronically with a stylus, finger, or mouse. Cf. *Mayton v. Tempoe, LLC*, No. SA-17-CV-179-XR, 2017 WL 2484849, at *4 (W.D. Tex. June 7, 2017) (concluding that the defendants had carried their burden of demonstrating that plaintiff had agreed to arbitration by signing his name on an electronic pen pad).

²³ See *Realogy Holdings Corp. v. Jongebloed*, 957 F.3d 523, 527 & n.1, 528, 532 (5th Cir. 2020) (upholding the district court’s finding that a former employee had agreed to various post-employment, noncompetition provisions in a so-called “clickwrap” agreement).

²⁴ TEX. BUS. & COM. CODE § 322.005(b).

²⁵ *Id.* § 322.009(a).

²⁶ *Id.*

acknowledgment procedures.”²⁷ Thus, security procedures may include requiring personal identifying information—such as a social security number or an address—to register for an account;²⁸ assigning a unique identifier to a user and then tying that identifier to the user’s actions;²⁹ maintaining a single, secure system for tracking user activities that prevents unauthorized access to electronic records;³⁰ business rules that require users to complete all steps in a program before moving on or completing it;³¹ and timestamps showing when users completed certain actions.³² These examples are illustrative and not exclusive under Section 322.009(a). The efficacy of the security procedure provides the link between the electronic record stored on a computer or in a database and the person to whom the record is attributed. A record that cannot be created or changed without unique, secret credentials can be attributed to the one person who holds

²⁷ *Id.* § 322.002(13). Relatedly, the Legislature defined an electronic record as any “record created, generated, sent, communicated, received, or stored by electronic means.” *Id.* § 322.002(7). A “record” is merely “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” *Id.* § 322.002(12).

²⁸ See *Butler v. Z&H Foods, Inc.*, No. 4:19-CV-02759, 2021 WL 630942, at *3 (S.D. Tex. Jan. 29, 2021) (concluding that the plaintiffs’ affidavits denying that they electronically signed an arbitration agreement did not raise a fact issue where the defendant introduced their employment files with “completed electronic employment applications containing personal details”, “digitally signed [Arbitration] Agreements”, and forms “contain[ing] social security numbers, digitally signed on the same day as the Agreements”); *Thick v. Dolgencorp of Tex., Inc.*, No. 4:16-CV-00733, 2017 WL 108297, at *2 (E.D. Tex. Jan. 11, 2017) (same).

²⁹ See *Rosales v. Coca-Cola Sw. Beverages LLC*, No. EP-18-CV-361-PRM, 2019 WL 1493359, at *7 (W.D. Tex. Apr. 3, 2019) (concluding that the defendant had met the requirements of § 322.009(a) by demonstrating that “employees enter unique employee identification numbers when they access electronic modules during the onboarding process”).

³⁰ See *Fries Rest. Mgmt., LLC v. Silva*, No. 13-18-00596-CV, 2020 WL 4381994, at *3 (Tex. App.—Corpus Christi July 30, 2020, pet. filed) (concluding that the evidence conclusively demonstrated the existence of a valid arbitration agreement where the defendant presented uncontroverted testimony that it exclusively used a specific online system for hiring employees and that it would have been impossible for the plaintiff to be added to payroll without the plaintiff’s having electronically signed the arbitration agreement).

³¹ See *id.*

³² See *GC Servs. L.P. v. Little*, No. H-19-1180, 2019 WL 5425032, at *6 (S.D. Tex. Oct. 23, 2019) (finding that the plaintiff had electronically signed the Dispute Resolution Agreement where her “timeline conflict[ed] with the timestamped documents and the credible evidence showing GC Services’[] usual application procedures”).

those credentials.

The Employees do not disagree. They concede that they completed Aerotek's computerized hiring application and electronically signed the documents included—save for one, the MAA. Aside from their denials, they offered no evidence to support their allegation that they did not electronically sign the MAAs that Aerotek introduced into evidence. Instead, they simply argue that Aerotek's evidence fell short of establishing the efficacy of the hiring application's security procedures. According to the Employees, the trial court was free to disregard Aerotek's witnesses.

Aerotek's evidence showing the security procedures its hiring application used to verify that a candidate electronically signed his MAA was uncontroverted. To enter the application, a candidate was required to create for himself a unique identifier, a user ID, a password, and security questions, all unknown to Aerotek. The candidate was required to enter personal information and sign documents by clicking on them. The application recorded and timestamped the candidate's every action. The application's business rules made it so that the application could not be submitted until all steps were completed and all required signatures provided, including on the MAA. Once a candidate submitted his application, Aerotek could not modify its contents. Aerotek provided the signed MAAs marked with timestamps identical to those in its database records showing each Employee's progress through the application.

The Employees argue that Marsh did not testify that it was impossible to complete the hiring application without signing the MAA, but that was exactly her testimony. Asked whether there was "any possible way" she could "imagine" that happening, she answered, "[n]ot with this process." Marsh explained that every part of the application had to be "signed and completed"

before the application could be “finalize[d] and submit[ted]”—statements backed up by her in-court demonstration of the very hiring application that the Employees used. The Employees argue that their signatures could have been added after their applications were completed. Again, Marsh testified to the contrary: “[w]e don’t have the ability to alter [forms] after they’re submitted” by a candidate. The Employees argue that Marsh’s in-court demonstration of the application showed only how it had worked *that day*, not how it worked when they used it. But Marsh specifically testified that the hiring application process had not changed since the Employees used it. The Employees argue that the application they used may have had a glitch. But Marsh testified that the only time a glitch occurred was when a server went offline and a candidate could not immediately respond to his invitation to use the system. The Employees argue that no evidence supports a finding that they signed the MAAs because Marsh did not “observe” them doing so. But Marsh did not need to observe them because the hiring application did, invisibly storing in a database an electronic record of each action the Employees took.

The Employees argue that testimony from a computer programmer, or at least an IT expert, was required to prove the application’s operation and security procedures. But Marsh testified that she had helped develop the application and managed its use in hundreds of thousands of instances. She was sufficiently familiar with the hiring application to give testimony on its actual operation. The Employees argue that Marsh was an interested witness whose testimony the trial court was free to discount. “Testimony by an interested witness may establish a fact as a matter of law only if the testimony could be readily contradicted if untrue, and is clear, direct and positive, and there are no circumstances tending to discredit or impeach it.”³³ Marsh’s testimony was certainly “clear,

³³ *Lofton v. Tex. Brine Corp.*, 777 S.W.2d 384, 386 (Tex. 1989) (citation omitted).

direct, and positive”. The Employees argue that their four affidavits averring that they never saw nor signed the MAA have a collective weight that discredits Aerotek’s evidence. But Marsh explicitly testified that the hiring application’s business rules would have prevented them from completing the hiring process without their signing the MAAs. Moreover, the Employees could have requested forensic tests of the hiring application to show that it did not operate as Marsh described, but they did not.

In addition, Allen argues that Sybil Harper, the Aerotek employee who assisted him with his hiring application, must have signed his MAA without his consent. But Harper testified that she routinely uses a “very strict” and “very structured” process for assisting candidates with the hiring application, having helped candidates over “a hundred times” as she sat “next to” them. From retrieving Aerotek’s welcome email, to “creat[ing] a user name and password”, to inputting “biographical information”, to signing the “arbitration agreement”, Harper testified that she makes sure that “[e]verything is entered” and “signed electronically”. And at “each step as [they] go through the process” Harper gets renewed “consent” to continue. Allen does not argue that Harper acted any differently in assisting him. For the same reason, his argument that Harper’s testimony lacks probative value since she does not specifically remember assisting him falls short. More importantly, he asserts with the other three Employees that he intended to complete the hiring application, which could not have been done without his signing the MAA.

The Employees also contend that Aerotek’s evidence cannot be conclusive for other reasons. The Employees argue that their “printed name[s]” on the MAAs cannot qualify as “a signature of any kind—not an actual signature or even an electronic signature.” But both our

caselaw, for wet-ink signatures,³⁴ and Section 322.002(8), for electronic signatures,³⁵ plainly provide otherwise. The Employees argue that Aerotek cannot conclusively prove they electronically signed the MAAs because “people onboarding with Aerotek can, from anywhere, create their ID and password, and can also login from anywhere.” In addition to proving too much,³⁶ that argument does not account for Aerotek’s evidence, which conclusively established that the only way a person could access each Employee’s information was through a secret combination of unique user ID, password, and security questions known only to the Employee. The Employees complain that Aerotek’s prevailing here would establish “an irrebuttable presumption” that electronic signatures on corporate records are valid. That is simply untrue. The Employees were free to seek discovery to discredit Aerotek’s evidence. They chose not to. Rather than attacking the reliability of the hiring application’s security procedures with evidence of their own, they chose to rely on mere argument. Because arguments are not evidence,³⁷ no evidence supports the Employees’ contentions.

Finally, we cannot agree with the dissent’s suggestion that merely denying an electronic

³⁴ It has long been the law in this State that “any mark” can qualify as a person’s signature, including a simple cross mark. *Cf. Howard v. Colquhoun*, 28 Tex. 134, 138 (1866); *see also Bustillos v. State*, 213 S.W.2d 837, 841 (Tex. Crim. App. 1948) (“To sign, in the primary sense of the word, is to make any mark. To sign an instrument or document is to make any mark upon it in token of knowledge, approval, acceptance, or obligation.” (quoting *In re Walker’s Estate*, 42 P. 815, 816 (Cal. 1895))) (cleaned up).

³⁵ The Legislature defined *electronic signature* as any “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.” TEX. BUS. & COM. CODE § 322.002(8).

³⁶ If, as the Employees contend, electronic signatures are invalid merely because a computer application is accessible “from anywhere”, then nearly every electronic signature made today would lack validity, including the typed signature by the Employees’ counsel on their electronically filed briefs in this Court.

³⁷ *See Kindred v. Con/Chem, Inc.*, 650 S.W.2d 61, 63 (Tex. 1983) (“When the evidence offered to prove a vital fact is so weak as to do no more than create a mere surmise or suspicion of its existence, the evidence is no more than a scintilla and, in legal effect, is no evidence.” (citations omitted)); *see also Cary v. State*, 507 S.W.3d 761, 766 (Tex. Crim. App. 2016) (noting that “arguments are not evidence” in a legal-sufficiency analysis (citation omitted)).

signature qualifies as some evidence in showing an electronically signed arbitration agreement's invalidity. The dissent makes much of the Commission of Appeals' decision in *Ward v. Weaver*,³⁸ a 90-year-old case in which we approved the Commission's recommendation that judgment on a verdict failing to find that Mrs. Weaver signed a deed be affirmed.³⁹ Whatever *Ward*'s continued validity is today, it does not control here.

For starters, the case is not binding on this Court. As we have explained many times, "our approval of the judgment recommended by the Commission . . . is not to be construed as an approval by the Supreme Court of the opinion of the Commission in the particular case, or the reasons given in the Commission's opinion for its conclusion."⁴⁰ And even if the case were binding, it dealt with circumstances materially different from those now before us. By allegedly signing a deed in ink, Mrs. Weaver did not opt into a statutory framework such as the one that the Act provides for electronic signatures, as Aerotek and the Employees did. Under Section 322.009's framework for electronic-signature attribution, once Aerotek proved its security procedures, the burden shifted to the Employees to demonstrate how their electronic signatures could have wound up on the MAAs without their having placed them there themselves. Mere denials do not suffice. As the dissent agrees, evidence cannot be disregarded when it "demonstrates 'physical facts that cannot be denied,' so that 'reasonable people could not differ in their conclusions.'"⁴¹ Aerotek's

³⁸ 34 S.W.2d 1093 (Tex. Comm'n App. 1931, judgment affirmed).

³⁹ *Id.* at 1094–1095; *see also post* at 1–2 ("But Mrs. Weaver swore under oath that neither she nor anyone authorized to act on her behalf had ever signed the deed. . . . [T]he Commission of Appeals agreed that Mrs. Weaver's sworn denial created a fact issue This Court agreed as well." (citations omitted)).

⁴⁰ *McKenzie v. Withers*, 109 Tex. 255, 256 (1918); *see also Provident Life & Accident Ins. Co. v. Knott*, 128 S.W.3d 211, 217 n.7 (Tex. 2003) ("[T]his Court's approval of the Texas Commission of Appeals' decision in *Johnson* did not indicate our agreement with its reasoning." (citations omitted)).

⁴¹ *Post* at 6 (quoting *City of Keller v. Wilson*, 168 S.W.3d 802, 815–816 (Tex. 2005)).

evidence did exactly that.

In sum, Aerotek’s evidence of the security procedures for its hiring application and its operation is such that reasonable people could not differ in concluding that the Employees could not have completed their hiring applications without signing the MAAs. The Employees’ simple denials are no evidence otherwise.

III

We agree with the dissenting Justices in the court of appeals that the significance of this case extends far beyond the parties’ dispute.⁴² As Texans continue to move online, the pace of innovation and change in everyday life continues to accelerate. When it comes to social interaction, some commentators suggest that as many as 72% of *all* Americans use social media to interact online.⁴³ Although “applying old doctrines” to these interactions “is rarely straightforward”,⁴⁴ it would be even less so if the electronic contracts governing them—terms of use or service, in many cases—were unnecessarily invalidated. When it comes to access to justice, the courts today are likewise heavily dependent on electronic signatures. For instance, our power to hear this case turns on the validity of the electronic, typed signatures that counsel submitted in their briefs.⁴⁵ And the same is true for commerce. The United States Census Bureau estimates that as many as 14% of all retail sales in 2020 happened online—up 32.4% from 2019—and all of them involved a contractual

⁴² 598 S.W.3d 373, 374 (Tex. App.—Dallas 2020) (Schenck, J., dissenting from the denial of reh’g en banc).

⁴³ *Social Media Fact Sheet*, PEW RES. CTR. (Apr. 7, 2021), <https://www.pewresearch.org/internet/fact-sheet/social-media/>.

⁴⁴ *Biden v. Knight First Amend. Inst. at Columbia Univ.*, 593 U.S. ___, 141 S. Ct. 1220, 1221 (2021) (Thomas, J., concurring).

⁴⁵ See TEX. R. APP. P. 9.1(c) (“A document that is electronically served, filed, or issued by a court or clerk is considered signed if the document includes . . . a ‘/s/’ and name typed in the space where the signature would otherwise appear . . .”).

exchange of some sort.⁴⁶ Our policymaking branch of government, the Legislature, has expressly declared it to be the policy of this State to facilitate those transactions.⁴⁷ Courts cannot unnecessarily stand in the way of the Legislature’s attempts to keep pace with that innovation.

Moreover, the Legislature is not the only policymaking body trying to keep pace: so, too, is Congress. In 2000, Congress enacted the Electronic Signatures in Global and National Commerce Act (the E-SIGN Act).⁴⁸ Section 7001 expressly provides that “with respect to any transaction in or affecting interstate or foreign commerce . . . a contract relating to such transaction may not be denied legal effect, validity, or enforceability because an electronic signature or electronic record was used in its formation.”⁴⁹ States may “modify, limit, or supersede” Section 7001 “only if” their changes are either consistent with the Uniform Electronic Transactions Act or the E-SIGN Act itself.⁵⁰ Because online interactions increasingly affect “interstate” and “foreign commerce”, courts must be wary of construing the Act in a way that raises preemption’s

⁴⁶ *Quarterly Retail E-Commerce Sales*, U.S. CENSUS BUREAU (Feb. 19, 2021, 10:00 AM), https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

⁴⁷ For instance, the Legislature expressly provided in Section 322.006 that:

[The Act] must be construed and applied:

- (1) to facilitate electronic transactions consistent with other applicable law;
- (2) to be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and
- (3) to effectuate its general purpose to make uniform law with respect to the subject of this chapter among states enacting it.

TEX. BUS. & COM. CODE § 322.006; *see also id.* § 322.007(b) (“A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.”).

⁴⁸ Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. ch. 96).

⁴⁹ 15 U.S.C. § 7001(a)(2).

⁵⁰ *Id.* § 7002(a)(1)–(2).

specter.

It may be that the use of electronic contracts already exceeds the use of paper contracts or that it will soon. The Act does not limit the ways in which electronic contracts may be proved valid, but it specifically states that proof of the efficacy of the security procedures used in generating a contract can prove that an electronic signature is attributable to an alleged signatory.⁵¹ An opposing party may, of course, offer evidence that security procedures lack integrity or effectiveness and therefore cannot reliably be used to connect a computer record to a particular person. But that attribution cannot be cast into doubt merely by denying the result that reliable procedures generate.

* * * * *

Aerotek conclusively established that the Employees signed, and therefore consented to, the MAAs, and the trial court erred in denying Aerotek's motion to compel arbitration. The judgment of the court of appeals is reversed, and the case is remanded to the trial court for further proceedings.

Nathan L. Hecht
Chief Justice

OPINION DELIVERED: May 28, 2021

⁵¹ See TEX. BUS. & COM. CODE § 322.009(a).