Electronic Signatures Are BINDING

A LOOK AT RECENT CASELAW.

WRITTEN BY **PIERRE GROSDIDIER**

THE AUTHENTICITY OF DIGITAL ACTS BY INDIVIDUALS is a recurring courtroom issue. Ten years ago, the Texas Court of Criminal Appeals set the standard for ascribing a text message or a social media posting to a person.[1] Recently, in *Aerotek, Inc. v. Boyd,* the Texas Supreme Court applied the Uniform Electronic Transactions Act, or UETA,[2] to uphold the validity of an arbitration agreement that former employees claimed they never digitally signed.[3]

Aerotek used an online application to recruit employees. Applicants accessed the application via their assigned unique username, password, and security questions. The application led each candidate through a workflow that required consent via digital signatures at certain steps. The first digital signature bound the applicant to "Aerotek's electronic hiring documents 'as though . . . signed . . . in writing.'" Another digital signature bound the applicant to a Mutual Arbitration Agreement, or MAA. Each action in the workflow created an unalterable record in the application's database, and applicants had to complete all steps to complete their employment application.[4]

Plaintiffs—employees hired and quickly terminated—sued Aerotek and others for racial discrimination and retaliation. Aerotek filed a motion to compel arbitration supported by copies of time-stamped records showing that plaintiffs electronically signed the MAA. Plaintiffs, in response, admitted that they completed the online hiring application but submitted sworn declarations that they had never "seen, signed, or been presented with the MAA." The trial court denied Aerotek's motion to compel arbitration and a divided 5th Court of Appeals in Dallas affirmed. Applying the UETA, the Texas Supreme Court reversed and remanded.[5]

The UETA "applies only to transactions between parties each of which has agreed to conduct transactions by electronic means."[6] It states in part that:

> [a]n electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.[7]

The UETA further defines a security procedure as:

> a procedure employed for the purpose of verifying that an electronic signature, record . . . is that of a specific person . . . [and] includes a procedure that requires the use of . . . identifying words or numbers, . . . or other acknowledgment procedures.[8]

The Texas Supreme Court found that Aerotek's security procedures featuring secret credentials qualified under this statutory language. It also found that the plaintiffs provided no evidence to support their claims other than their declarations and that they sought no discovery from Aerotek to discredit its evidence.[9]

The court rejected the plaintiffs' attempts to impeach the testimony of the Aerotek program manager who defined and helped design and develop the application. She had testified, inter alia, that the employees could not have completed their application without signing the MAA and that Aerotek had no ability to alter the employees' submitted records. Importantly, the court rejected the plaintiffs' argument that the testimony of an IT expert was required "to prove the application's operation and security procedures."[10] The program manager had helped develop the application and had overseen its use by "hundreds of thousands" of applicants. She was, therefore, sufficiently qualified to testify regarding its operation, and her testimony was "sufficiently 'clear, direct, and positive'" to overcome her interested witness status.[11] In light of this evidence, the court held that "reasonable people could not differ in concluding that the Employees could not have completed their hiring applications without signing the MAAs."[12] Consequently, the trial court's factual finding that the plaintiffs did not sign the MAAs was not supported by the evidence and merited no deference. **TBJ**

This article, which was originally published in Circuits, *has been edited and reprinted with permission.*

NOTES

1. *See Tienda v. State,* 358 S.W.3d 633, 641–42 (Tex. Crim. App. 2012) (requiring something more than phone or account ownership to ascribe a text message or a post to a person, even if the bar for this "something more" is low); *see also, "Authenticating: can cellphone text messages stand up in court?"* Texas Bar Journal, April 2016, p. 278.
2. Tex. Bus. & Comm. Code §§ 322.001 *et seq.*
3. 624 S.W.3d 199, 200 (Tex. 2021).
4. *Id.* at 201.
5. *Id.* at 202–04.
6. Tex. Bus. & Comm. Code § 322.005(b).
7. *Id.* § 322.009(a).
8. *Id.* § 322.002(13).
9. *Aerotek,* 624 S.W.3d at 208.
10. *Id.* at 207.
11. *Id.*
12. *Id.* at 209.

PIERRE GROSDIDIER is an attorney in Houston. He belongs to the first group of attorneys certified in construction law by the Texas Board of Legal Specialization in 2017. Grosdidier's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, he worked in the process control industry. Grosdidier holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a fellow of the American Bar Foundation, and the State Bar of Texas Computer and Technology Section chair for 2022-2023.