Received: 7/10/2020 3:38 PM

IN THE

INDIANA SUPREME COURT

Case No. _____

COMMUNITY HEALTH NETWORK, INC. Appellant, v. HEATHER McKENZIE and DANIEL McKENZIE, individually and as parents and natural guardians of J.M. and O.M., JOHN McKENZIE, DEBORAH WEST, MICHAEL WEST, and KATRINA GRAY, Appellees.	)	Appeal from the Marion Superior Court Trial Court Cause No. 49D04-1401-CT-433 The Honorable Cynthia J. Ayers, Judge Court of Appeals Case No. 19A-CT-873

INDIANA STATE MEDICAL ASSOCIATION AND AMERICAN MEDICAL ASSOCIATION'S *AMICI CURIAE* BRIEF IN SUPPORT OF PETITION TO TRANSFER

Libby Yin Goodknight
KRIEG DeVAULT LLP
One Indiana Square, Suite 2800
Indianapolis, Indiana 46204-2079
Telephone: (317) 636-4341
Facsimile: (317) 636-1507
E-mail: lgoodknight@kdlegal.com

Attorney for *Amici Curiae*
Indiana State Medical Association
and American Medical Association

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

STATEMENT OF INTEREST

The Indiana State Medical Association ("ISMA") is an association of approximately 8,500 physicians and medical students across the State of Indiana whose mission is to maximize the leadership and impact of physicians. ISMA provides continuing medical education for its member physicians so they may deliver the best possible health care to their patients. ISMA represents the collective interests of its member physicians on matters of public policy and works to foster a better understanding of physicians and health care issues in the community, in the Legislature and state administrative agencies, and in the courts.

The American Medical Association ("AMA"), through the Litigation Center of the AMA and state medical societies, is the voice of America's medical profession in legal proceedings around the country. AMA is the largest professional association of physicians, residents, and medical students in the United States. Additionally, through state and specialty medical societies and other physician groups seated in its House of Delegates, substantially all U.S. physicians, residents, and medical students are represented in AMA's policy-making process. AMA's members practice in all areas of medical specialization and in every state, including Indiana.

As representatives of Indiana's health care community, ISMA and AMA (collectively, "*Amici*") have a strong interest in the outcome of this appeal and, in particular, the issue of respondeat superior that is presented on transfer. This issue stems from an action brought against Community Health Network, Inc. ("Community") and its former employee, Katrina Gray ("Gray"), based on Gray's

unauthorized access of Plaintiffs' medical records. The trial court denied summary judgment on Plaintiffs' claim against Community alleging respondeat superior liability, finding a question of fact as to whether Gray's unauthorized access of Plaintiffs' medical records fell within the scope of her employment. The Court of Appeals affirmed that ruling in *Community Health Network, Inc. v. McKenzie*, ___ N.E.3d ___, 2020 WL 2666588, at *10-11 (Ind. Ct. App. May 26, 2020).

The Court of Appeals' analysis of respondeat superior against the backdrop of a health care employee's unauthorized access of medical records is deeply concerning to *Amici* and their member health care providers. *Amici* have a unique appreciation for, and can offer a valuable perspective on, the implications for all health care providers in Indiana if the Court of Appeals' erosion of respondeat superior principles is allowed to stand. *Amici* urge the Court to grant transfer and vacate the Court of Appeals' opinion on this issue.

SUMMARY OF ARGUMENT

With the passage of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the proliferation of electronic medical records under the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009, it is now standard practice for health care providers to mandate that their employees sign confidentiality agreements expressly prohibiting the access, use, and disclosure of patient health information for personal or non-business reasons. Health care providers require employees to sign such agreements as a condition of their employment, establishing from the onset that the unauthorized access of medical

records is decidedly *outside* the scope of their employment. This is what Community did when it hired Gray, and her confidentiality agreement should have foreclosed Plaintiffs' claim alleging respondeat superior liability as a matter of law.

But the Court of Appeals discounts how important employee confidentiality agreements are to the delivery of health care in the digital – and highly-regulated – age of electronic medical records. Indeed, the Court of Appeals dismisses *Robbins v. Trustees of Indiana University*, 45 N.E.3d 1 (Ind. Ct. App. 2015), and never mentions *Hayden v. Franciscan Alliance, Inc.*, 131 N.E.3d 685 (Ind. Ct. App. 2019), *trans. denied*, two cases in which the panels rightly determined as a matter of law that the hospital employees' unauthorized access of medical records was *not* within the scope of their employment under the specific terms of their confidentiality agreements. Instead, the Court of Appeals follows *Walgreen Co. v. Hinchy*, 21 N.E.3d 99 (Ind. Ct. App. 2014), *clarified on reh'g*, *trans. denied*, despite "no evidence that the pharmacist in *Hinchy* signed a confidentiality agreement . . . ." *See Hayden*, 131 N.E.3d at 692 (distinguishing *Hinchy* on this basis).

The Court of Appeals compounds its disregard for the significance of confidentiality agreements to the scope of employment inquiry – especially in the health care context – by concluding that even though Gray indisputably "misused employer-conferred power and authority to access" Plaintiffs' medical records, whether she was acting within the scope of her employment is still a question of fact

because she "was authorized to use her assigned desktop computer with Epic[1] and other software to access patient health information." *McKenzie*, 2020 WL 2666588 at *11. A health care employee's mere access to a computerized EMR system like Epic does not – and should not – automatically create a question of fact as to whether her unauthorized access of medical records was within the scope of her employment. Such an outcome contravenes long-standing Indiana precedent and oversimplifies the realities of modern medicine. If health care providers are vicariously exposed every time an employee accesses a patient's health information using her work computer – whether job-related or not – this will subject providers to unnecessary and prolonged litigation without serving the policies underlying respondeat superior liability.

ARGUMENT

I. Employee Confidentiality Agreements In The Health Care Industry Make The Unauthorized Access Of Medical Records For Personal Or Non-Business Reasons Decidedly Outside The Scope Of Employment.

It has been nearly 25 years since HIPAA was passed in the early days of electronic medical records. Congress enacted HIPAA in 1996 to protect the privacy and security of health information transmitted electronically. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. Under HIPAA, the U.S. Department of Health and Human Services developed regulations that set national standards for the protection of a patient's individually identifiable

[1] Epic is a proprietary electronic medical record ("EMR") software application that is used by health care providers and hospital systems throughout the country and around the world. There are several other companies that compete with Epic in the provision of EMR products and services.

health information. 45 C.F.R. §§ 164.102, 164.306. In 2009, Congress enacted the HITECH Act to promote the use of electronic medical records and the development of a nationwide health information technology infrastructure as a means of improving the delivery and quality of patient care. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001, 123 Stat. 115, 230; *see also* 42 U.S.C. § 300jj-11(b). The HITECH Act expanded the privacy and security requirements under HIPAA and increased the penalties for HIPAA violations. Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, §13001, 123 Stat. 226; *see also* 45 C.F.R. § 164.404.

Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions is a "covered entity" that must comply with HIPAA. 45 C.F.R. § 164.104(a); *see also* 45 C.F.R. § 160.103. Pursuant to 45 C.F.R. § 164.306(a)(1), covered entities must "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity . . . creates, receives, maintains, or transmits." Moreover, the covered entity must "[e]nsure compliance [with these requirements] by its workforce." 45 C.F.R. § 164.306(a)(4).

To that end, the "covered entity must train all members of its workforce on the policies and procedures with respect to protected health information . . . ." 45 C.F.R. § 164.530(b)(1). This training must occur "within a reasonable period of time after [any person] joins the covered entity's workforce . . . ." 45 C.F.R. § 164.530(b)(2)(i)(B); *see also* 45 C.F.R. § 164.308(a)(5)(i). In addition, the "covered entity must have and

apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements" under HIPAA. 45 C.F.R. § 164.530(e)(1); *see also* 45 C.F.R. § 164.308(a)(1)(ii)(C).

It is within this medical-legal framework that it has become standard practice for health care providers to mandate that their employees sign confidentiality agreements expressly prohibiting the access, use, and disclosure of patient health information for personal or non-business reasons. The hospital in *Robbins* required its employee to sign a confidentiality agreement in which she agreed she could "only access, use . . . , or disclose information for which [she had] a business reason and [was] authorized to do so" and promised that "[a]t no time [would she] access, use, or disclose confidential or sensitive information . . . for a personal, unauthorized, unethical, or illegal reason." 45 N.E.3d at 4. The hospital in *Hayden* required its employee to sign a confidentiality agreement in which she agreed she could only "use and access information that [was] needed to perform [her] job duties" and acknowledged that "inappropriate use or disclosure of information on [her] part [could] result in . . . personal liability." 131 N.E.3d at 692.

In this case, Community also required Gray to sign a confidentiality agreement at the outset of her employment. (App. Vol. V at 74, 96.) Under the terms of her confidentiality agreement, Gray professed her "understand[ing] that patient information . . . [was] to be considered confidential" and acknowledged she could "only view and share patient information that [was] necessary to perform [her] job . . . ."

(App. Vol. V at 96.) Gray further agreed to "be held accountable for [her] own actions and [her] failure to . . . maintain confidentiality . . . ." (App. Vol. V at 96.)

When health care providers like Community and the hospitals in *Robbins* and *Hayden* require their employees to sign confidentiality agreements as a condition of their employment, this establishes from the onset that the employees' unauthorized access of medical records for personal or non-business reasons is decidedly *outside* the scope of their employment. Such agreements strike a crucial balance between the accessibility of medical records vital to the delivery of patient care and patients' privacy interests in their individually identifiable health information.[2] Such agreements have the additional effect of defining the precise nature and extent of the employer-employee relationship, which is the sole source of any respondeat superior liability. *See Hinchy*, 21 N.E.3d at 107 ("An employer is not held liable under the doctrine of respondeat superior because it did anything wrong, but rather 'because of the [employer's] relationship to the wrongdoer.'") (quoting *Sword v. NKC Hosps., Inc.*, 714 N.E.2d 142, 148 (Ind. 1999)) (alteration in original); *see also Warner Trucking, Inc. v. Carolina Cas. Ins. Co.*, 686 N.E.2d 102, 105 (Ind. 1997) ("The critical inquiry" is whether "employee's act originated in activities so closely associated with the employment relationship as to fall within its scope.") (internal quotations and citation omitted).

[2] Under HIPAA, a covered entity must simultaneously ensure the confidentiality and the availability of all electronic protected health information. 45 C.F.R. § 164.306(a)(1). One of the purposes of the HITECH Act's nationwide health information technology infrastructure is to "improve[] the coordination of care and information" across a continuum of health care providers. 42 U.S.C. § 300jj-11(b)(6).

Employee confidentiality agreements thus serve an important function in today's digital – and highly-regulated – health care environment. While a health care employee may be authorized to access patient health information *for the purpose of performing her job*, she is "expressly *not authorized* to access, use, or disclose the information for personal, unauthorized, unethical, or illegal reasons." *Hayden,* 131 N.E.3d at 692 (quoting *Robbins*, 45 N.E.3d at 10). Other courts agree. *See, e.g., Bagent v. Blessing Care Corp.*, 862 N.E.2d 985, 994 (Ill. 2007) (explaining that "employer's prohibition [against the unauthorized disclosure of medical records] accentuates the limits of the employee's permissible action and . . . supports a finding that the prohibited act is entirely beyond the scope of employment"); *Korntved v. Advanced Healthcare, S.C.*, 704 N.W.2d 597, 603-04 (Wis. Ct. App. 2005) (ruling that confidentiality policy signed as condition of employment "expressly state[d] that accessing [medical] records for non-work purposes [was] prohibited" and was therefore outside the scope of employment).

Notably, whether a health care provider can be found *directly* liable in the presence of a confidentiality agreement has no bearing on whether it can – or should – be held *vicariously* liable under the doctrine of respondeat superior. *But see Robbins*, 45 N.E.3d at 14 (Crone, J., concurring). Strict adherence to an employee's defined scope of employment as set forth in her confidentiality agreement is all the more important when assessing vicarious liability against an employer. Unlike direct liability, "[a]n employer is not held liable under the doctrine of respondeat superior because it did anything wrong . . . ." *Hinchy*, 21 N.E.3d at 107.

As in *Robbins* and *Hayden*, Gray's confidentiality agreement with Community defined the outer limits of their relationship and should have foreclosed Plaintiffs' claim alleging respondeat superior as a matter of law. Unfortunately, the Court of Appeals disregards the sound rationale and medical realities of *Robbins* and *Hayden*, choosing instead to follow the result reached in *Hinchy*. In so doing, the Court of Appeals ignores the absence of any "evidence that the pharmacist in *Hinchy* signed a confidentiality agreement" – a critical distinction that was properly emphasized in both *Robbins* and *Hayden*. *Hayden*, 131 N.E.3d at 692; *Robbins*, 45 N.E.3d at 11.

The Court of Appeals attempts to diminish the importance of the confidentiality agreement in *Robbins*, implying that it was really the employee's federal guilty plea and affidavit that were outcome determinative. *McKenzie*, 2020 WL 2666588 at * 11. Putting aside this misreading of *Robbins*, it is inappropriate to suggest that summary judgment is impossible in a respondeat superior action without such a heightened level of evidence. Not all – indeed, very few – cases involving the unauthorized access of medical records are going to result in federal criminal charges, let alone guilty pleas. *See United States v. Scott*, 631 F.3d 401, 406 (7th Cir. 2011) (recognizing that prosecutorial decisions can involve all sorts of "factors such as the strength of the case, the prosecution's general deterrence value, [and] the Government's enforcement priorities") (internal quotations and citation omitted).

Moreover, an affidavit from Gray would have been entirely duplicative of Community's other designated evidence. Gray had already agreed under the terms of

her confidentiality agreement that she could "only view and share patient information that [was] necessary to perform [her] job[,]" (App. Vol. V at 96), and Plaintiffs "had not received care or services at the [orthopedic center where Gray worked]" – meaning that her access of Plaintiffs' medical records had nothing to do with the performance of her job. *McKenzie*, 2020 WL 2666588 at *2. Plaintiffs themselves asserted in their Amended Complaint that Gray accessed their medical records "without a business need" for doing so, thereby eliminating any question of fact for the jury. (App. Vol. II at 60.)

In short, this Court should grant transfer and uphold the significance of confidentiality agreements to the scope of employment inquiry – especially in the health care context.

II. A Health Care Employee's Mere Access To A Computerized EMR System Does Not Automatically Create An Issue Of Fact As To Whether The Unauthorized Access Of Medical Records Was Within The Scope of Employment.

The Court of Appeals also concludes that, even though Gray indisputably "misused employer-conferred power and authority to access" Plaintiffs' medical records, whether she was acting within the scope of her employment is still a question of fact because she "was authorized to use her assigned desktop computer with Epic and other software to access patient health information." *McKenzie*, 2020 WL 2666588 at *11. In essence, the Court of Appeals considers a health care employee's mere access to a computerized EMR system like Epic as automatically creating a question of fact as to whether the unauthorized access of medical records was within

the scope of her employment. The Court of Appeals' logic conflicts with Indiana precedent and oversimplifies the analysis.

"It has long been settled that mere use of the employer's facilities to commit a wrongful act . . . do[es] not[,] without more[,] [bring the act within the scope of employment or] present a sufficient nexus [to the employee's job duties] to merit [a] decision by the fact-finder." *City of Indianapolis v. West*, 81 N.E.3d 1069, 1074-75 (Ind. Ct. App. 2017). Just "because an act could not have occurred without access to the employer's facilities does not bring it within the scope of employment" either. *Konkle v. Henson*, 672 N.E.2d 450, 457 (Ind. Ct. App. 1996). "The question is not whether the employer's facilities were used, but what the facilities were used *for*, and whether such use was sufficiently associated with the employee's ordinary employment use." *West*, 81 N.E.3d at 1075; *see also Ware v. Bronson Methodist Hosp.*, No. 307886, 2014 WL 5689877, at *3 (Mich. Ct. App. Nov. 4, 2014) (fact that employee accessed patient files "by using her employee identification number in the manner in which she normally accessed patient files during her daily work" did not establish she was acting within scope of employment; employer is not liable "merely because the existence of the employment relationship made it easier for employee to accomplish a tort").

In *Doe v. Lafayette School Corporation*, the Court of Appeals affirmed summary judgment for a school corporation on the question of vicarious liability for a teacher's sexual molestation of a student. 846 N.E.2d 691, 702 (Ind. Ct. App. 2006), *abrogated on other grounds by State Farm Mut. Auto. Ins. Co. v. Jakupko*, 881 N.E.2d 654 (Ind.

2008). The teacher sent e-mails to the student during school hours using his school-issued laptop computer. *Id.* at 695. Nevertheless, the teacher's actions fell outside the scope of his employment because he was not authorized to send personal e-mails to students or pursue a romantic relationship with a student. *Id.* at 702.

In *West*, the Court of Appeals reversed the denial of summary judgment for the City of Indianapolis on a claim of respondeat superior. The plaintiff argued that the City was vicariously liable for its employee's use of her work computer and e-mail address to send a purportedly defamatory email about the plaintiff. The Court of Appeals determined that the e-mail was not sent within the scope of employment even though the employee's "use of her City-issued computer and e-mail address was central to the performance of her employment duties." *West,* 81 N.E.3d at 1075. The Court of Appeals pronounced that "[m]odern offices could not function without [e-mail]. [To hold] employers vicariously liable for every e-mail their employees send from a work e-mail account – whether job-related or not – would risk an avalanche of litigation against employers without serving the policies underlying vicarious liability." *Id.* (internal quotations and citation omitted). This astute observation applies with equal force in this case.

"The purpose of the doctrine [of respondeat superior] is to properly allocate the economic costs of doing business." *Shelby v. Truck & Bus. Grp. Div. of Gen. Motors Corp.*, 533 N.E.2d 1296, 1298 (Ind. Ct. App. 1989). "A business benefits from its employees performing their work within the scope of their employment. Thus, when another party is injured as the result of an employee performing work within the

scope of his employment, the doctrine requires that the business pay the attendant costs which accompany the benefit." *Id.* (citation omitted); *see also Stump v. Ind. Equip. Co.*, 601 N.E.2d 398, 403 (Ind. Ct. App. 1992) (stating that doctrine is premised on the notion that "he who expects to derive advantage from an act which is done by another for him must answer for any injury which a third person may sustain from it") (citation omitted).

Modern medical offices and health care facilities could not function without computerized EMR systems that, in turn, must be physically accessed by employees using employer-issued computers.[3] If a health care employee's normal job duties entail accessing patient health information, she will likely be assigned a work computer, loaded with EMR software, that enables her to retrieve that information and perform her job. But if health care providers are vicariously exposed *every* time an employee accesses a patient's health information using her work computer – whether job-related or not – this will subject providers to unnecessary and prolonged litigation without serving the policies underlying respondeat superior liability. *See West*, 81 N.E.3d at 1075.

[3] In the federal Government's view, patient care would suffer in the absence of such systems. *See, e.g.,* 42 U.S.C. § 300jj-11(b)(2) (promoting development of nationwide health information technology infrastructure to "improve[] health care quality, reduce[] medical errors, . . . and advance[] the delivery of patient-centered medical care"); *see also* Press Release, The White House, President Discusses Health Care in State of the Union (Jan. 20, 2004), georgewbush-whitehouse.archives.gov/news/releases/2004/01/20040120-11.html ("By computerizing health records, we can avoid dangerous medical mistakes, reduce costs and improve care.").

In computerized EMR systems, each patient's unique medical file is separately and securely maintained from every other patient's unique medical file. One patient's medical file cannot be accessed through any portals in another patient's medical file. Information in each patient's medical file is captured, classified, and coded at various points over the course of the patient's treatment. Each patient's medical file may contain a wide range of information in a variety of electronic formats and subfiles, including patient demographics; medical and medication histories; vital signs; progress notes and charts; lab results; radiological images such as X-Rays, CT Scans, MRIs, and Mammographs; .wav files of EEGs and EKGs; invoices; and health insurance claims.

When a health care employee uses her work computer to deliberately access a patient's unique medical file housed in an EMR system for personal or non-business reasons, there is no accompanying "benefit" or "advantage" to her employer derived from this conduct. *See Shelby*, 533 N.E.2d at 1298; *Stump*, 601 N.E.2d at 403. There is nothing about the employee's conduct that "further[s] the employer's business." *See Barnett v. Clark*, 889 N.E.2d 281, 283 (Ind. 2008). And there is nothing about the employee's conduct that is "intermingled with authorized job duties" or remotely "incidental to the conduct authorized" by her employer.[4] *See Hinchy*, 21 N.E.3d at 107, 111. Each separate act of searching for, locating, and viewing a patient's discrete

[4] *SoderVick v. Parkview Health System, Inc.*, is distinguishable to the extent the employee in *SoderVick*, unlike Gray, was specifically authorized to be in the plaintiff's chart for the purpose of entering information from the patient's information worksheet. ___ N.E.3d ___, 2020 WL 2503923, at *1 (Ind. Ct. App. May 15, 2020).

health information for personal or non-business reasons requires an intentional series of keystrokes and actions "occur[ing] within an independent course of conduct not intended by the employee to serve any purpose of the employer." *See Barnett*, 889 N.E.2d at 284 (emphasis removed, citation omitted). This is the very definition of an act falling *outside* the scope of employment.

This is particularly true when the health care employee has signed a confidentiality agreement that expressly prohibits her from accessing, using, and disclosing a patient's health information for personal or non-business reasons. When an employee signs such an agreement as a condition of her employment, it cannot be said that her unauthorized access of medical records "arise[s] naturally or predictably from the activities [she] was hired or authorized to do . . . ." *See Cox v. Evansville Police Dep't*, 107 N.E.3d 453, 462 (Ind. 2018); *see also Cannady v. St. Vincent Infirmary Med. Ctr.*, 537 S.W.3d 259, 265 (Ark. 2018) (holding that employees' unauthorized access of medical records in violation of confidentiality agreements and federal law could not "be expected given the nature of the job"). Quite the opposite, when an employee is "not explicitly or impliedly authorized to access or disclose medical records for personal reasons" under the terms of a confidentiality agreement, "her actions [are] *not* an extension of [the] authorized access" the health care provider afforded her at the outset. *Robbins*, 45 N.E.3d at 11 (emphasis added).

Here, Gray's ability to access *certain* medical records necessary to perform her job was not, as a matter of law, sufficiently associated with her unauthorized access of *Plaintiffs'* medical records. *See Hayden*, 131 N.E.3d at 692 ("Although Collins was

authorized to use Franciscan's computer to look up patient records, she was not authorized to do so for personal reasons."); *Doe*, 846 N.E.2d at 702 (Although "[school] authorized Cole to send emails to students for school purposes, there is no indication that [school] authorized him to send emails to students for personal reasons."). Indeed, it is uncontroverted that Plaintiffs never "received care or services" in the orthopedic center at Community where Gray worked.[5] *McKenzie*, 2020 WL 2666588 at *2. Gray's mere access to Community's EMR system through a Community-provided desktop computer does not – and should not – create a question of fact as to whether her unauthorized access of Plaintiffs' medical records was within the scope of her employment. The Court of Appeals' holding otherwise erodes Indiana's respondeat superior principles and reduces the scope of employment inquiry to a piece of hardware.

CONCLUSION

For the foregoing reasons, *Amici* respectfully request the Court grant transfer and vacate the Court of Appeals' opinion on the issue of respondeat superior.

[5] This contrasts with the pharmacist in *Hinchy*, who actually worked at the plaintiff's local pharmacy where she filled her prescriptions. 21 N.E.3d at 105.

Respectfully submitted,

/s/ Libby Yin Goodknight
Libby Yin Goodknight, Attorney No. 20880-49
KRIEG DeVAULT LLP
One Indiana Square, Suite 2800
Indianapolis, Indiana 46204-2079
Telephone: (317) 636-4341
Facsimile: (317) 636-1507
E-mail: lgoodknight@kdlegal.com

Attorney for *Amici Curiae*
Indiana State Medical Association
and American Medical Association

WORD COUNT CERTIFICATE

The undersigned counsel verifies that the foregoing *Amicus Curiae* Brief in Support of Petition to Transfer (excluding cover page, table of contents, table of authorities, word count certificate, certificate of service, and signature block) contains 4,198 words as determined by the word count of the word processing system used to prepare this Brief, specifically Microsoft Word, which is no more than the 4,200 words permitted by Indiana Appellate Rule 44(E).

/s/ Libby Yin Goodknight
Libby Yin Goodknight

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the foregoing has been served electronically upon the following counsel of record through the Indiana E-filing System (IEFS) this 10th day of July, 2020:

Sherry A. Fabina-Abney
Jenny R. Buchheit
Stephen E. Reynolds
Sean T. Dewey
ICE MILLER LLP
One American Square, Suite 2900
Indianapolis, Indiana 46282

William N. Riley
James A. Piatt
Joseph N. Williams
Anne Medlin Lowe
RILEY WILLIAMS & PIATT, LLC
The Hammond Block Building
301 Massachusetts Avenue
Indianapolis, Indiana 46204

G. Jayson Marksberry
MARKSBERRY LAW OFFICES LLC
1185 Northfield Drive, Suite B
Brownsburg, Indiana 46112

/s/ Libby Yin Goodknight
Libby Yin Goodknight

KD_(10895845.5).docx