No. 21-2763

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

TYLER GUTTERMAN, *ET AL.*,
APPELLANTS

v.

INDIANA UNIVERSITY BLOOMINGTON, *ET AL.*,
APPELLEES

Appeal from the United States District Court
for the Southern District of Indiana, Indianapolis Division
Cause No. 1:20-cv-02801-JMS-MJD
The Honorable Jane Magnus-Stinson, Judge

BRIEF OF APPELLEES INDIANA UNIVERSITY, BLOOMINGTON, AND PAMELA S. WHITTEN, IN HER OFFICIAL CAPACITY AS PRESIDENT OF INDIANA UNIVERSITY

Jenny R. Buchheit (counsel of record)
Sean T. Dewey
ICE MILLER LLP
One American Square, Suite 2900
Indianapolis, IN 46282-0200
(317) 236-2295 (telephone)
(317) 592-5487 (facsimile)
jenny.buchheit@icemiller.com
sean.dewey@icemiller.com

Attorneys for Appellees Indiana University, Bloomington, and Pamela S. Whitten, in her official capacity as President of Indiana University

AMENDED APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 21-2763

Short Caption: Tyler Gutterman, et al. v. Indiana University Bloomington, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervener or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Trustees of Indiana University (misnamed in Plaintiffs' Complaint and this appeal as Indiana University Bloomington, Indiana)

and Pamela S. Whitten, in her official capacity as President of Indiana University

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Ice Miller LLP

(3) If the party, amicus or intervener is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervener's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ *Jenny R. Buchheit* Date: 12/8/2021

Attorney's Printed Name: Jenny R. Buchheit

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes X No

Address: Ice Miller LLP

One American Square, Suite 2900, Indianapolis, IN 46282-0200

Phone Number: (317) 236-2295 Fax Number: (317) 594-5487

E-Mail Address: jenny.buchheit@icemiller.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 21-2763

Short Caption: Tyler Gutterman, et al. v. Indiana University Bloomington, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervener or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Trustees of Indiana University (misnamed in Plaintiffs' Complaint and this appeal as Indiana University Bloomington, Indiana)

and Pamela S. Whitten, in her official capacity as President of Indiana University

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Ice Miller LLP

(3) If the party, amicus or intervener is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervener's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ *Sean T. Dewey* Date: 12/8/2021

Attorney's Printed Name: Sean T. Dewey

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes ____ No X

Address: Ice Miller LLP

One American Square, Suite 2900, Indianapolis, IN 46282-0200

Phone Number: (317) 236-2198 Fax Number: (317) 592-4694

E-Mail Address: sean.dewey@icemiller.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGES**

STATUTES **PAGES**

RULES **PAGES**

OTHER AUTHORITIES **PAGES**

JURISDICTIONAL STATEMENT

Appellants (Plaintiffs below) brought this lawsuit against Appellees, Trustees of Indiana University, misnamed in Appellants' Complaint as Indiana University, Bloomington, and Pamela S. Whitten, in her official capacity as President of Indiana University (collectively, "IU" or the "University"), asserting that IU's limited review of historic data from their student ID cards constituted an unreasonable search and seizure in violation of the Fourth and Fourteenth Amendments of the United States Constitution, and sought relief under 42 U.S.C. § 1983. Appellants also alleged that IU's review of their data violated a breach of their contract with the University. (*See generally* Dkt. 1.)

The United States District Court for the Southern District of Indiana had jurisdiction over Appellants' search and seizure claims (Counts I and II of the Complaint) pursuant to 28 U.S.C. § 1331, because they arose under the Fourth and Fourteenth Amendments to the United States Constitution, and 28 U.S.C. § 1343, because Appellants sought relief under 42 U.S.C. § 1983. The district court had pendent jurisdiction over Appellants' state law breach of contract claim (Count III of the Complaint) pursuant to 28 U.S.C. § 1367.

This Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291. The district court granted the University's Motion to Dismiss Appellants' Complaint in its entirety on September 1, 2021 (Dkt. 50), and entered Final Judgment, which disposed of all claims as to all parties, on September 1, 2021 as well (Dkt. 51). There were no motions for a new trial, to alter the judgment, or for any other relief that

tolled the time within which to appeal. Appellants timely filed their notice of appeal on September 24, 2021.

STATEMENT OF THE ISSUE

IU issues CrimsonCards to all faculty, staff, and students—including Appellants—which are used to, among other things, access University services and facilities, including residence halls. During the course of an investigation into whether Appellants' fraternity was hazing its freshman pledges, IU accessed limited CrimsonCard data from the fraternity's pledge class—including Appellants—to confirm they were not the victims of hazing. Appellants later filed this lawsuit, claiming IU's actions constituted an unreasonable search in violation of the Fourth Amendment, because their CrimsonCard data was accessed without their consent.

Did the district court correctly determine that even if a search occurred, such a search was reasonable and did not violate the Fourth Amendment, as Appellants did not plausibly allege that IU's use of the CrimsonCard data was unreasonable, and IU had a legitimate purpose for accessing the data to ensure the safety of its students—including Appellants—by confirming they were not subjected to hazing?

STATEMENT OF THE CASE

IU is a public research university. (Dkt. 1 at 2.) In the fall of 2018, Appellants were freshmen completing their first semester of study at IU's Bloomington, Indiana campus. (*Id.* at 3.) All four of them chose to pledge the same Greek fraternity, Beta Theta Pi. (*Id.*)

IU's CrimsonCards

IU issues a "CrimsonCard Photo ID" (the "CrimsonCard") to its students and employees. (*Id.*; *see also* Dkt. 20-1, "CrimsonCard Terms and Conditions"[1].) The CrimsonCard "is the property of [IU]." (Dkt. 20-1.) It "is much more than a photo ID. It's a print release card, keycard to authorized university buildings, library card, and if you're enrolled in a dining services plan, it's your meal ticket." (Dkt. 1 at 4) (citation and quotation omitted).

The reverse side of the CrimsonCard contains a magnetic stripe, along with the following text:

INDIANA UNIVERSITY

If found, please contact: (317) 274-0400

Manage your account online: crimsoncard.iu.edu

> Use of this card constitutes acceptance of the CrimsonCard terms and conditions. This card is the property of Indiana University and is intended for use only by Indiana University and its affiliates. Unauthorized use, lending, or tampering with the card warrants confiscation and/or disciplinary action.

[1] Because Appellants' Complaint referred to the CrimsonCard, and to certain of IU's policies, including the CrimsonCard Terms and Conditions, the district court considered them in connection with the Motion to Dismiss. (*See* Dkt. 50 at 4 n.2) (citing *Adams v. City of Indianapolis*, 742 F.3d 720, 729 (7th Cir. 2014)).

(Dkt. 20 at 11.)

The CrimsonCard Terms and Conditions, which are referenced on the back of the CrimsonCard, provide that:

> The CrimsonCard … is issued by [IU] to its students and employees, and others associated with [IU], to verify their identity and manage access to [IU] services and facilities.
>
> The Card also functions as a stored value card, and is associated with an account, the "CrimsonAccount—CrimsonCash."
>
> * * *
>
> This Agreement is entered into between [IU] and each student … .
>
> In exchange for being issued a Card, Cardholder agrees to abide by the *Official University Identification Card Policy* (available on the University Policies website at http://policies.iu.edu) (the "Policy") and to the following terms and conditions:
>
> * * *
>
> **Use and Ownership**
>
> *Cardholder understands and agrees that the Card is the property of [IU].*
>
> * * *
>
> **Damaged, Lost, Stolen, Misused or Expired Cards**
>
> Cardholder is responsible for care and protection of the Card. If the magnetic stripe, of any of the technology contained in or on the card, is damaged and becomes unreadable by any Card reader or terminal, Cardholder is required to obtain a replacement of the Card at Cardholder's expense …

(Dkt. 20-1 at 2-3) (emphasis added).

The referenced *Official University Identification Card Policy*, or UA-13, provides:

Policy Statement

[IU] issues Photo Identification Cards … to employees, students, and others associated with [IU] to verify their identity and manage their access to [IU] services and facilities.

The ID card will be used to verify the identity of the bearer of the card in [IU] facilities when such identification is needed to be present at those facilities or on [IU] grounds.

* * *

Official University Identification Card

1. The University recognizes the Official University Identification Card as official identification for use of University services, facilities, and other purposes described in this policy.

* * *

4. Identification information collected for production of the Official University Identification Card may be used by the University to support the safety and security of campus resources and support the mission of the University. Release of this information is governed by Management of Institutional Data Policy (DM-01) and may require approval by the appropriate data steward or data manager.

* * *

Intended Use of the Official University Identification Card

* * *

2. The Official University Identification Card is intended for use as an electronic identification, validation, and authentication credential for authorized access to services and facilities. The Official University Identification Card *is the property of the University* and will be deactivated and/or invalidated by the University upon expiration of its intended use.

* * *

4. The Official University Identification Card may be used to verify the identity of the bearer of the card while on University grounds.

(Dkt. 20-2 at 4-6) (emphasis added).

Finally, the Management of Institutional Data Policy (DM-01) provides:

> **Scope**
>
> This policy applies to all users of [IU] information and information technology resources regardless of affiliation, and irrespective of whether these resources are accessed from on-campus or off-campus locations.
>
> This policy applies to all institutional data, and is to be followed by all those who capture data and manage administrative information systems using university assets.
>
> **Policy Statement**
>
> * * *
>
> The permission to access institutional data should be granted to all eligible employees and designated appointees of the university for all legitimate university purposes.

(Dkt. 20-3 at 4.)

Appellants claim they are "required to carry their CrimsonCard as a condition of their attendance at IU, and IU retains historical records of [their] CrimsonCard usage." (Dkt. 50 at 3.) According to Appellants, IU maintains records which "track every time a student 'swipes' his [CrimsonCard] to gain access to a university building or to use a university facility" (hereinafter "Swipe Data"). (Dkt. 1 at 4.) As the district court summarized, this "Swipe Data" purportedly

> includes the whole range of students' movements and activities, including access to dorm buildings, individual dorm rooms, elevators, and dorm building common areas. The Swipe Data also reflects students' movements around campus, including checking out library books, accessing academic buildings, accessing parking garages, using parking meters, purchasing meals at university dining halls, purchasing sodas and snacks from campus and vending machines,

> using laundry machines, printing materials they need for class on university printers, and other daily activities. The Swipe Data is not limited to campus facilities, as the Crimson Card operates as a payment card at numerous businesses near campus, including restaurants, grocery stores, pharmacies, airport shuttles, tanning salons, and wellness centers. The subject of a search of Swipe Data is not given "the opportunity to obtain precompliance review before a neutral decisionmaker."

(Dkt. 50 at 6) (citations omitted).

IU's Hazing Investigation of Beta Theta Pi

During the fall 2018 semester, IU began investigating allegations that Beta Theta Pi was hazing its pledges. (Dkt. 1 at 3-4.) As part of its investigation, IU accessed Appellants' Swipe Data, to "compar[e] their 'swipe' data to their testimony as to their whereabouts at the time of the incident." (*Id.* at 4.) Appellants had informed IU they were in their dorm rooms at the time of the suspected hazing. (*Id.*) Although Beta Theta Pi was ultimately sanctioned, Appellants were not penalized or otherwise found guilty of any wrongdoing. (*Id.*)

Proceedings Below

On October 29, 2020, Appellants filed suit against IU and President Whitten, in her official capacity only, asserting that IU and President Whitten had violated Appellants' rights under the Fourth and Fourteenth Amendments to the United States Constitution by using their Swipe Data to track their movements (Count I) and by retaining their Swipe Data and accessing it without providing them an "opportunity to obtain precompliance review before a neutral decisionmaker" (Count II), and had breached their contract with Appellants by using the Swipe Data to track Appellants' movements (Count III). (Dkt. 1 at 10-12.) Appellants sought

nominal damages, declaratory relief, and attorneys' fees and costs, and requested that the district court enjoin IU from "further use of swipe data in investigations except where [IU] has obtained a warrant or can demonstrate exigent circumstances," and require IU to "expunge the investigation for which [IU] used swipe data of [Appellants] from their permanent records, to the extent that [Appellants]' records include information about such investigation." (*Id.* at 13.)

IU and President Whitten moved to dismiss Appellants' Complaint in its entirety, pursuant to Fed. R. Civ. P. 12(b)(6), arguing that with the exception of Appellants' claims for prospective injunctive relief against President Whitten, the Complaint was barred by the Eleventh Amendment, as IU had not waived its sovereign immunity or consented to this lawsuit. (Dkt. 20 at 6-7.) They also argued Appellants' claims for prospective injunctive relief must fail, as IU's actions did not constitute a "search" for purposes of the Fourth Amendment, and even if it was a "search," such a search was reasonable under the circumstances. (*Id.* at 9-20.)

On September 1, 2020, the district court issued its Order on IU's Motion to Dismiss (Dkt. 50). First, it agreed that IU and President Whitten were entitled to sovereign immunity for Appellants' constitutional claims (Counts I and II), and granted the Motion to Dismiss, to the extent those claims sought monetary or declaratory relief. (*Id.* at 10.) The district court then addressed Appellants' constitutional claims against President Whitten for prospective injunctive relief—the only constitutional claims remaining—and found that even if a search occurred (it assumed, without deciding, that one did), such a search was reasonable. (*Id.* at

16.) Thus, it granted the Motion to Dismiss Counts I and II in their entirety, with prejudice. (*Id.* at 18.)

The district court declined to exercise supplemental jurisdiction over Appellants' breach of contract claim (Count III), and dismissed it without prejudice. (*Id.* at 19.) Final judgment was entered against Appellants and in favor of IU and President Whitten that same day. (Dkt. 51.) Appellants timely filed their Notice of Appeal on September 24, 2021. (Dkt. 52.)

SUMMARY OF ARGUMENT

IU values and protects the privacy of its students, as well as their records, in accordance with University policy and the law. IU has over 40,000 students on its Bloomington campus, and the health, safety, and education of those students are of paramount importance to the University. Accordingly, IU takes very seriously reports of hazing and will take action to help protect students from such behavior.

Appellants' Complaint (Dkt. 1) stems from IU's alleged verification of limited data from their CrimsonCards—i.e., their Student ID cards—during the course of a hazing investigation involving their fraternity. This data was accessed to confirm members of Appellants' pledge class had not been victims of hazing by the fraternity, and although the fraternity was ultimately sanctioned, no adverse action was taken against Appellants, who remain undergraduate students at IU's Bloomington campus. Despite this fact, Appellants allege violations of the Fourth Amendment's prohibition against unreasonable searches.

The district court correctly determined Appellants' constitutional claims (Counts I and II) fail, and their lawsuit against the University should be dismissed. Quite simply, there was no "search" which violated their Fourth Amendment privacy interests. There was no entry into Appellants' dorm rooms, nor do Appellants have a reasonable expectation of privacy in the CrimsonCard data IU accessed, as both the CrimsonCards and the data generated by them are the property of the University.

Moreover, even if there was a "search" for purposes of the Fourth Amendment (there wasn't), such a search was reasonable. Appellants were well aware of the purpose and capabilities of the CrimsonCard—to access IU's services and facilities—and specifically agreed to the Terms and Conditions of the CrimsonCard, which spelled out IU's ownership of the card. As such, they cannot reasonably have expected their use of the CrimsonCard to remain private.

Here, IU acted within its authority to respond to allegations of hazing and to help protect members of its student body, including Appellants—an interest the district court found to be "plainly legitimate." Not only did IU access limited CrimsonCard data (residence hall entry), it did so for a limited time period (the time of the alleged hazing incident). And contrary to Appellants' contentions on appeal, the focus of IU's investigation remained Appellants' fraternity—Appellants were never a subject of the investigation, and they were never disciplined or found guilty of any wrongdoing. Rather, their data was accessed only to confirm they were not victims of hazing.

The district court correctly concluded that even if a search occurred, such a search was reasonable and did not violate Appellants' Fourth Amendment rights. Its Judgment in favor of the University and against Appellants should be *affirmed*.

ARGUMENT

I. Standard of Review

This Court's review of a district court's ruling on a motion to dismiss is *de novo*. *Smith v. City of Chicago,* 3 F.4th 332, 335 (7th Cir. 2021) (internal citation omitted). The complaint must "set forth a claim that is plausible on its face, that is, to contain enough facts to draw the reasonable inference that the defendant is liable." *Nelson v. City of Chicago,* 992 F.3d 599, 603 (7th Cir. 2021) (cleaned up). While this Court "draw[s] all reasonable inferences and facts in the favor of the nonmovant, [it] need not accept as true any legal assertions or recital of the elements of a cause of action supported by mere conclusory statements." *Vesely v. Armslist LLC,* 762 F.3d 661, 664-65 (7th Cir. 2014) (internal quotation omitted). And in reviewing the district court's ruling, this Court "may affirm the decision on any ground supported by the record." *Jones v. Cummings,* 998 F.3d 782, 785 (7th Cir. 2021) (internal citation omitted).

II. The district court correctly determined IU's use of its CrimsonCard data did not violate Appellants' Fourth Amendment rights.

As set forth in *U.S. v. Thompson,* 811 F.3d 944, 948 (7th Cir. 2016), a search occurs either when the government "physically intrudes without consent upon a constitutionally protected area" or "when an expectation of privacy that society is

prepared to consider reasonable is infringed." (internal quotations omitted). Any Fourth Amendment analysis must, therefore, begin "by specifying precisely the nature of the state activity that is challenged." *Smith v. Maryland,* 442 U.S. 735, 741 (1979). Appellants have not done so here.

In their Brief, as they did below (*see* Dkt. 50 at 12-13), Appellants incorrectly frame their Fourth Amendment analysis around the *interior* of their dorm rooms. But there are simply no allegations which support any inference that IU searched or entered Appellants' dorm rooms[2] or otherwise "invade[d] students' privacy in the most intimate of spaces, their home, [using] modern technology … ." (Appellants' Br. at 21.)

Rather, here, IU accessed limited, specific CrimsonCard data, relating only to the time of the alleged hazing incident, to determine when Appellants accessed their residence halls. IU did so as part of its investigation into whether members of Appellants' pledge class were the victims of hazing by their fraternity. While it is IU's position that this access wasn't a "search," for purposes of the Fourth Amendment, as the district court noted below, "when an alleged search is not

[2] Because the University never *physically* entered Appellants' residence halls, let alone their dorm rooms, Appellants' argument that the Fourth Amendment extends beyond one's dorm room and into the hallway and other common areas is inapplicable. (*See* Appellants' Br. at 7.) That's because the protection afforded a home's curtilage applies only under a traditional trespass analysis of the Fourth Amendment. *See U.S. v. Jones,* 565 U.S. 400, 410-11 (2012); *see also Florida v. Jardines,* 569 U.S. 1, 10-11 (2013) (noting *Katz* is inapplicable where government physically intrudes). Conversely, "[s]ituations involving merely the transmission of electronic signals without trespass *would* remain subject to *Katz* analysis." *Jones,* 565 U.S. at 411 (emphasis original). Because this case involves IU's review of limited CrimsonCard data, the "reasonable expectation of privacy" analysis enunciated by *Katz v. U.S.*, 389 U.S. 347 (1967), and its progeny controls.

performed as part of a criminal investigation, the Court may 'turn immediately to an assessment of whether [the search is] reasonable.'" (Dkt. 50 at 14) (quoting *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2015)).

In assessing reasonableness, the Court "look[s] to the totality of the circumstances, balancing the degree to which the search intrudes on individual liberty and the degree to which it promotes legitimate governmental interests." *U.S. v. White,* 781 F.3d 858, 862 (7th Cir. 2015) (citing *Wyoming v. Houghton,* 526 U.S. 295, 300 (1999)). This necessitates consideration of "one's status and privacy expectations and the context in which the search occurs." (Dkt. 50 at 14) (quoting *U.S. v. Wood,* 426 F. Supp. 3d 560, 565-66 (N.D. Ind. 2019)); *see also Medlock v. Trustees of Ind. Univ.,* 738 F.3d 867, 872 (7th Cir. 2013) (citing *New Jersey v. T.L.O.,* 469 U.S. 325, 340 (1985)) (recognizing unique needs of school setting). Here, the district court correctly determined that IU's access of Appellants' limited, specific CrimsonCard data, which related only to the time of the hazing incident,[3] was reasonable, and thus, did not violate Appellants' Fourth Amendment rights. The district court's Judgment should be affirmed.

[3] In their Complaint, Appellants alleged that "IU officials accessed the historical records of [Appellants'] [CrimsonCards] to track [Appellants'] movements." (Dkt. 1 at 3, ¶ 15.) Appellants further alleged that IU "used [the data] to check the alibis of several students—including [Appellants]—after an alleged off-campus hazing incident by comparing their 'swipe' data to their testimony as to their whereabouts at the time of the incident." (*Id.* at 4, ¶ 18.)

A. Appellants do not have a Fourth Amendment privacy interest in IU's institutional data.

Because Appellants "were on notice that the CrimsonCard was used to access IU's services and facilities, and that IU owned the card, it is not reasonable to conclude that [Appellants] expected their use of the CrimsonCard—which, in turn, reflected which IU facilities and services they accessed—to be private." (Dkt. 50 at 14.) As the district court explained, IU owns all CrimsonCards, and as such, the data contained on those CrimsonCards (or generated by them) constitutes "institutional data" under IU's DM-01 policy. (*See* Dkt. 20-1 at 2-3: "Cardholder understands and agrees that the Card *is the property of the University*." (emphasis added); *see also* Dkt. 20-2 at 3: "The [Crimson]Card is the property of the University and will be deactivated and/or invalidated by the University upon expiration of its intended use.") IU's DM-01 policy prescribes when the University or its employees may access institutional data and the appropriate uses of institutional data. (*See* Dkt. 20-3 at 3; *see also* Dkt. 20-2 at 5 (providing that CrimsonCard identification information "may be used by the University to support the safety and security of campus resources and support the mission of the University.").)

IU did not violate Appellants' Fourth Amendment rights by accessing its own institutional data in accordance with University policy. (*See* Dkt. 50 at 5-6) (highlighting relevant portions of IU's DM-01 policy). Specifically, DM-01 provides that "permission to access institutional data should be granted to all eligible employees and designated appointees of the university for all legitimate university

purposes." (*Id.* at 6.) In this case, as Appellants themselves allege,[4] IU accessed limited CrimsonCard data to protect the safety and well-being of its students, specifically—to ensure that Beta Theta Pi's freshman pledge class (including Appellants themselves) were not victims of hazing by their fraternity, an interest the district court found to be "plainly legitimate." (*Id.* at 16.)

"The law is clear: no person has a legitimate expectation of privacy in the business-records of an entity with whom business has been conducted and, therefore, has no interest protected by the Fourth Amendment." *U.S. v. Simmons*, 569 F. Supp. 1155, 1157 (M.D. Tenn. 1983) (listing cases). Such records include checks and deposit slips, *U.S. v. Miller,* 425 U.S. 435 (1976); loan-guarantee agreements, *U.S. v. Payner*, 447 U.S. 727 (1980), *reh'g denied*; an employee's employment records with his employer*, Donaldson v. U.S.*, 400 U.S. 517 (1971); the numbers dialed on a telephone, *Smith*, 442 U.S. at 740-41; residential utility records, *U.S. v. McIntyre*, 646 F.3d 1107, 1111-12 (8th Cir. 2011) (collecting cases); credit card records, *U.S. v. Phibbs,* 999 F.2d 1053, 1077-78 (6th Cir. 1993); and, here, data from IU's CrimsonCards related to dorm access. Thus, as a matter of law, for purposes of the Fourth Amendment, Appellants did not have a legitimate expectation of privacy in their CrimsonCard data, which remains both the property and business records of IU.

[4] In their Complaint, Appellants admit that "as freshmen pledges, they would have been far more likely to be the victims of any hazing activity, rather than the perpetrators." (Dkt. 1 at 4, ¶ 19.)

B. IU's access of limited CrimsonCard data, in connection with its hazing investigation, was reasonable.

1. Society does not recognize as reasonable Appellants' claimed privacy interest in limited CrimsonCard Data.

Apart from the issue of data ownership and the capabilities of the CrimsonCard itself, as well as the information affirmatively communicated by the student to the University through the student's use of the CrimsonCard, "an individual has no reasonable expectation of privacy in public movements that he voluntarily conveyed to anyone who wanted to look." *Carpenter v. U.S.*, --- U.S. ----, 138 S.Ct. 2206, 2219-20 (2018) (quotation omitted). Stated differently, the Government only conducts a "search" for purposes of the Fourth Amendment where it tracks movements in private locations that could not otherwise be obtained by visual observation. *See Naperville*, 900 F.3d at 526 (citing *Kyllo v. U.S.*, 533 U.S. 27, 40 (2001)).

Here, the limited information accessed by IU—i.e., Appellants' access to their residence halls, could have been obtained by visual observation. Simply put, confirming whether or not Appellants entered their residence halls is not a "search," for purposes of the Fourth Amendment, as anyone (e.g., other students, RAs, investigators from IU's Office of Student Conduct, or police officers) could have visually observed them enter (or exit) their residence halls. And where the information learned is something that could have been seen by neighbors, law enforcement, or others passing by, it is not a "search." *See U.S. v. Tuggle,* 4 F.4th 505, 514 (7th Cir. 2021) (finding pole cameras capturing plaintiff's movements in and out of his home was not a Fourth Amendment violation and compiling cases);

see also U.S. v. Kelly, 385 F. Supp. 3d 721, 726-27 (E.D. Wis. 2019) (same with respect to cameras monitoring apartment building's entrance); *Chaney v. City of Albany,* 2019 WL 3857995, at *8-9 (N.D.N.Y. Aug. 16, 2019) (finding no Fourth Amendment violation where police reviewed logs of automatic license plate readers located at fixed locations around the city, which identified dates, times, and locations when plaintiff's car was observed).

2. Given the known capabilities of the CrimsonCard, it was unreasonable for Appellants to expect their use of the CrimsonCard to be private.

Appellants' claimed expectation of privacy in data generated by their CrimsonCard usage is belied by the CrimsonCard itself. As Appellants' Complaint acknowledges, the "CrimsonCard is much more than a photo ID. It's a print release card, keycard to authorized university buildings, library card, and if you're enrolled in dining services plan, it's your meal ticket." (Dkt. 1 at 4, ¶ 17) (citation and quotation omitted). Appellants cannot now claim to have a reasonable expectation of privacy in their use of the CrimsonCard, given that they were aware of the capabilities of the CrimsonCard, and its connection to both IU and University life, from the very beginning of their time on campus. As the district court explained:

> Given that [Appellants] were on notice that the CrimsonCard was used to access IU's services and facilities, and that IU owned the card, it is not reasonable to conclude that Appellants expected their use of the CrimsonCard—which, in turn, reflected which IU facilities and services they accessed—to be private … this is particularly true in today's day and age.

(Dkt. 50 at 14.)

To be sure, the conduct Appellants complain of—IU's review of limited data from the University-owned CrimsonCard to see whether Appellants "swiped" into their residence halls—is even less intrusive than the Government's actions in *Tuggle*, where this Court found no Fourth Amendment violation. There, police mounted three pole cameras on public property near plaintiff's home—two on a pole in the adjacent alleyway, which monitored the front of Tuggle's home, and a third camera, which also captured Tuggle's home and a shed owned by a co-conspirator. 4 F.4th at 511. The cameras recorded 24/7 for eighteen months, and officers had the ability to remotely "zoom, pan, and tilt the cameras" to enhance their view. *Id*. The footage revealed numerous suspected drug transactions and also captured individuals arriving at and departing from Tuggle's home. *Id.*

In arriving at its holding, the Court relied on two separate lines of cases. *First,* the Court looked to *Kyllo* and other enhanced-technology cases, concluding that "under a straightforward application of *Kyllo,* the isolated use of pole cameras [] did not run afoul of Fourth Amendment protections." *Id.* at 516. The Court specifically noted that cameras were in "general public use," and also explained that everything the government learned would have been visible by the naked eye and was "a far cry from the highly sophisticated surveillance equipment not generally available to the public." *Id.* (internal quotation omitted). *Second,* the Court looked to *Jones* and *Carpenter* in considering whether the prolonged, eighteen-month, around-the-clock surveillance violated the Fourth Amendment, ultimately concluding it did not. *Id.* at 518-29.

Here, as Appellants allege, the CrimsonCard is needed only to access an IU building or facility, including one's dorm. (Dkt. 1 at 4, ¶ 17.) The data generated, therefore, only reveals that a student *entered* the IU building or facility. Given there is no need to "swipe" out of an IU building or facility, including one's dorm, the data would not reveal if or when Appellants left their dorm room or the residence hall(s). And while *Tuggle* explains why this access of limited CrimsonCard data does not run afoul of the Fourth Amendment, the reasoning here is even more clear cut, as the level of intrusion is significantly less than the three pole cameras in that case.

The conduct Appellants complain of—reviewing limited data from the University-owned CrimsonCard to see whether Appellants "swiped" into their residence halls—is akin to the review of a telephone pen register, which chronologically logs the numbers dialed, and which does not violate the Fourth Amendment because such registers "do not acquire the *contents* of communications," but rather "disclose only the telephone numbers that have been dialed—a means of establishing communication," *Smith,* 442 U.S. at 741 (citation omitted) (emphasis original). Similarly, here, the CrimsonCard data only reveals if and when Appellants "swiped" into their residence hall(s), (Dkt. 1 at 4, ¶ 17), and does not reveal what Appellants did when they got there or how long they stayed.[5] Thus, like

[5] For example, if the CrimsonCard data showed that a student entered his or her residence hall at 10:00 p.m. on Friday evening and, again, at 10:00 a.m. on Saturday morning, IU would have no way to know whether the student stepped out at 9:55 a.m. to chat with a neighbor, returned from an hour's long run, or spent the night elsewhere. Nor would the data reveal whether the student held the door open for other students (who wouldn't have generated "swipe" data when entering).

the pen register in *Smith*, the CrimsonCard access log does not violate the Fourth Amendment.

Appellants predictably argue that CrimsonCard data is similar to the GPS device installed on a car's undercarriage in *Jones,* 565 U.S. at 402-03, which continuously established the car's location within 50 to 100 feet and relayed more than 2,000 pages of data over a 28-day period, or to the cell-site location information ("CSLI") at issue in *Carpenter*, 138 S.Ct. at 2212, which catalogued Carpenter's movements and triangulated his precise location with almost 13,000 location points over a four-month period. *See id.* at 2218 ("when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user"). Such a comparison is completely inappropriate.

In an attempt to shoehorn their argument into a *Carpenter*-style analysis, Appellants argue in their Brief that the University uses swipe data to "track[] [Appellants] all around campus: where and when they eat, sleep, do laundry, study, shop, and even go to the bathroom[6] … add[ing] up to a comprehensive portrait of their movements." (Appellants' Br. at 19.) Not only is this characterization vastly different from the allegations in their Complaint, that the University retained only a few months of data and used it for the limited purpose of checking their whereabouts "at the time of the [hazing] incident," (Dkt. 1 at 6, ¶ 18), which allegations must govern the Court's consideration of this Rule 12(b)(6) motion, *see Peterson v. Wexford Health Sources, Inc.,* 986 F.3d 746, 752 n.2 (7th Cir. 2021)

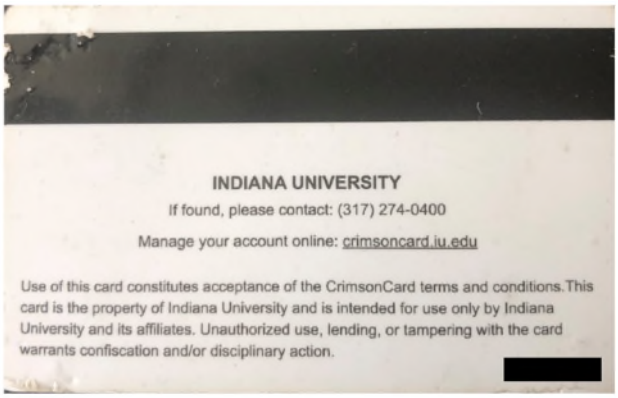
[6] The Complaint makes no allegation regarding collection of data regarding Appellants' bathroom use. (*See generally* Dkt. 1.)

(recognizing consideration of motion to dismiss is confined to well-pleaded facts in plaintiff's complaint and any elaborations made in opposing dismissal must be "consistent with the pleadings"), but the data generated by the CrimsonCard is distinguishable from CSLI in several important ways.

First, data stored on or generated by CrimsonCards is "institutional data" under IU's DM-01 policy. (*See* Dkt. 20-1 (CrimsonCard Terms and Conditions): "Cardholder understands and agrees that the Card *is the property of the University*." (emphasis added); *see also* Dkt. 20-2 at 3: "The [Crimson]Card is the property of the University and will be deactivated and/or invalidated by the University upon expiration of its intended use.") IU's DM-01 policy prescribes when the University or its employees may access institutional data and the appropriate uses of that data. Specifically, DM-01 provides that "permission to access institutional data should be granted to all eligible employees and designated appointees of the university for all legitimate university purposes." (*See* Dkt. 20-3 at 3.) In this case, only a few IU employees accessed the limited CrimsonCard data to investigate claims of hazing by a fraternity, which violate both University policy and Indiana law, and to protect the safety and well-being of IU's students (including Appellants), both of which are undoubtedly legitimate university purposes under IU's DM-01 policy. *See also Medlock,* 738 F.3d at 872 (recognizing special considerations in assessing reasonableness under Fourth Amendment for school settings).

Second, the CrimsonCard access data is more akin to the magnetic stripe data contained on credit cards, debit cards, or gift cards, which communicate

limited identifying information stored on the card to allow card users to make purchases, ATM withdrawals, confirm account information at one's bank, or access flight, hotel, or car rental reservations at self-service kiosks. Similarly, the CrimsonCard authenticates access to campus buildings and allows students wishing to take advantage of its conveniences to access their meal plan, rent library books, make debit-like purchases on campus or at participating off-campus locations by communicating limited data contained on the CrimsonCard's magnetic stripe to University readers or terminals to identify the user and validate their access or purchases. (*See* Official University Identification Card Policy, Dkt. 20-2 at 3) ("The [CrimsonCard] is intended for use as an electronic identification, validation, and authentication credential for authorized access to services and facilities.").



(Dkt. 20 at 11 (Exemplar CrimsonCard); *see also* Dkt. 50 at 4 n.2.)

The Fifth, Sixth, and Eighth Circuits have *all* considered and rejected the argument that a cardholder has a Fourth Amendment privacy expectation in identifying magnetic stripe data. *See U.S. v. Turner,* 839 F.3d 429, 436 (5th Cir. 2016) (concluding that "society does not recognize as reasonable an expectation of privacy in the information encoded in a gift card's magnetic stripe"); *U.S. v. Bah,*

794 F.3d 617, 631 (6th Cir. 2015) ("A credit card's stored information … is *intended* to be read by third parties. That is the only reason for its existence") (internal quotation omitted); *U.S. v. De L'Isle,* 825 F.3d 426, 432 (8th Cir. 2016) ("[T]he purpose of a credit, debit, or gift card is to enable the holder of the card to make purchases, and to accomplish this, the holder must transfer information from the card to the seller, which negates an expressed privacy interest"). This Court should join those circuits in rejecting Appellants' claim to the contrary with respect to the data generated by swiping the CrimsonCard's magnetic stripe. *See, e.g., Tuggle,* 4 F.4th at 522 (parting ways with sister circuits "generally requires quite solid justification; [and this Court] do[es] not lightly conclude that [its] sister circuits are wrong.") (quoting *Andrews v. Chevy Chase Bank,* 545 F.3d 570, 576 (7th Cir. 2008)).

Third, while Appellants seemingly suggest in their Brief that IU actively tracks *every* student as if the CrimsonCard is a GPS tracking device or surreptitiously pings to cell towers, the reality is the CrimsonCard provides a *single* data point for each physical "swipe" by the student.[7] (*See* Dkt. 1 at 4, ¶ 17.) Unlike

[7] Appellants' citation to *Karo, Kyllo,* and *Jardines* is unhelpful. (*See* Appellants' Br. at 14-15.) None of those cases, which discuss technologically enhanced emanations from a home's interior, are applicable here. *See U.S. v. Karo,* 468 U.S. 705, 715 (1984) (beeper emanating from home's interior captured by monitoring device); *Kyllo,* 533 U.S. at 34-35 (heat signatures emanating from home's interior captured by thermal imaging device); *Jardines,* 569 U.S. at 12 (odor of marijuana emanating from home's interior captured by trained narcotics dog); *see also Katz,* 389 U.S. at 358-89 (conversations emanating from phone booth captured by listening device). Not only is this argument different than the allegations in their Complaint (*see* Dkt. 1 at 4, ¶ 17), but, as explained above, a single "swipe" of the CrimsonCard only reveals that a student entered their residence hall or dorm room. It does not and cannot reveal whether they remained there (or what they did when inside). *See supra* note 5. Because the limited CrimsonCard data accessed provides no

CSLI, which can identify phones in the same geographical area, CrimsonCard swipe card data cannot identify when two or more people enter a building simultaneously (i.e., holding the door for a friend visiting one's dorm), nor would it capture instances where access occurs when a door is unlocked or left ajar. The CrimsonCard data cannot reveal how long a student stayed in their room (in contrast to the cameras in *Tuggle,* the CSLI in *Carpenter*, or the GPS device in *Jones*—all of which *do* reveal how long someone stays in a particular location). But most importantly, CrimsonCard data does not reveal where Appellants went once they were inside, what they did while inside, whether they invited anyone inside, when they went to sleep, if they made telephone calls, worked on the computer, watched television, etc.

Finally, CrimsonCard data does not show or reasonably demonstrate the purpose or intent of a student's access to an IU building or facility, which Appellants seem to suggest in their misguided attempt to argue that the capabilities of the CrimsonCard could be used for nefarious purposes.[8] *See, e.g., U.S.*

---

emanations from the dorm room's interior, *U.S. v. Knotts*, and not *Karo*, controls. *See Knotts,* 460 U.S. 276, 281-82 (1983) (finding no Fourth Amendment violation where visual surveillance from public spaces would have revealed same information to police and "the use of the beeper to signal the presence of [the] automobile to the police receiver, does not alter the situation"); a*ccord Tuggle,* 4 F.4th at 515-16.

[8] Appellants' exaggerated (and unsubstantiated) claim that "[a] hostile university administration could track which students attended meetings of the Federalist Society or Black Lives Matter; university employees would know who is going to the campus psychologist for counseling or to the campus clinic that test for sexually transmitted disease; they may have records of each evening students spent with their significant other (or were cheating on their significant other), including whether a closeted student is visiting a significant other of the same sex,"

v. Soybel, 13 F.4th 584, 593 (7th Cir. 2021) (rejecting defendant's argument that IP-address information, including websites visited like Credit Karma and Match.com, "provide[d] an 'intimate window' into his 'familial, political, professional, religious, and sexual associations' because the same was true of phone numbers captured by a pen register and, in any event, the government could not intercept content). As *Carpenter* explained, CSLI is unique because it can used to "track" multiple persons at very frequent intervals (perhaps revealing phone users frequently in close proximity to one another (and, thus, deducing associations), where they go, the routes they take, and how long they stay), regardless of whether one is actively using their smartphone. CrimsonCard data—as explained in detail herein—is a far cry from CSLI.

The analysis in *Heeger v. Facebook, Inc.,* 509 F. Supp. 3d 1182 (N.D. Cal. 2020), is helpful here. There, the court considered whether Facebook's *collection, storage and use* of plaintiffs' IP address information ran afoul of *Carpenter*, answering that question with an emphatic 'no'. *Id.* at 1190. As it explained, "[t]he collection of IP addresses is a country mile from the CSLI collected in *Carpenter*." *Id.* That's because "there is no legally protected privacy interest in IP addresses." *Id.* Further distinguishing *Carpenter*, the court reasoned that *Carpenter* was limited to the unique context of CSLI, noting that "cell-site location information data and IP addresses are apples and oranges for privacy purposes." *Id.* CSLI is "generated several times a minute whenever a cell phone's signal is on, even if the owner is not

---

(Appellants' Br. at 19-20), must be disregarded. This dystopian hypothetical has no basis in fact (nor is it alleged in Appellants' Complaint).

using one of the phone's features," which limits one's ability to opt out. *Id.* (cleaned up).

In contrast, while IP addresses can show location data, they were more "akin to a pen register recording the outgoing phone numbers dialed on a landline telephone," which "will not do for a privacy injury." *Id.* Despite Appellants' attempts to liken this case to the CSLI addressed in *Carpenter,* the *Heeger* court's analysis of the collection, storage, and use of IP addresses is a much more apt comparison to the CrimsonCard data at issue here. (*See* Dkt. 20 at 16-17.) The *Heeger* court's post-*Carpenter* analysis also mirrors this Court's conclusion that there is no reasonable expectation of privacy in one's IP address. *See Soybel,* 13 F.4th at 594; *U.S. v. Caira,* 833 F.3d 803, 806 (7th Cir. 2016).

In further contrast to *Carpenter*, here, CrimsonCard data is *not* continuously or involuntarily generated. Instead, Appellants generate CrimsonCard data only when they *voluntarily and physically use* their CrimsonCard at a reader or terminal to authenticate access to the building or room. Further unlike CSLI, Appellants can decide how much to limit their use of the CrimsonCard for non-essential functions, which affords one more opportunity to opt out. *See Heeger,* 509 F. Supp. 3d at 1189-90; *see also Soybel,* 13 F.4th at 593 ("We do not discount the importance of the internet in 2021. But it's not the case that Soybel created the data without any affirmative act beyond powering up. An internet user creates connection data by making the affirmative decision to access a website.") (cleaned up). Quite simply, this case is not *Carpenter* or *Naperville*, where there was no real choice at all.

Carpenter, 138 S.Ct. at 2220 (recognizing that a cell phone logs "cell-site record[s] by dint of its operation, without any affirmative act on the part of the user beyond powering up" and "there is no way to avoid leaving behind a trail of location data."); *Naperville,* 900 F.3d at 527 ("If [Naperville's residents] want electricity in their homes, they must buy it from the city's public utility. And they cannot opt out of the smart-meter program.").

Here, Appellants have multiple options to either limit generating swipe data or avoid it altogether. They can prioritize privacy over convenience by electing not to use their CrimsonCard for on- or off-campus purchases; opting to use cash or another payment method; opting to bring laundry to a laundromat; bringing their own printer instead of campus print stations; making their own meals or dining off campus; or living in off-campus housing. Even more obvious, Appellants could have also attended another college or university altogether. Therefore, to the extent that the CrimsonCard's "single datapoints add up to a comprehensive portrait of their movements," as Appellants argue (Appellants' Br. at 18), whether those paintings are detailed Rembrandts or abstract Picassos, is entirely of Appellants own choosing.

3. IU's access of CrimsonCard data was limited in both scope and time.

Moreover, as the district court highlighted, Appellants themselves alleged IU only retained the CrimsonCard data "for several months," (Dkt. 50 at 15), and even then, IU was only focused on the dates and times surrounding the hazing incident, and not looking at the entirety of those records. Thus, the facts alleged here are

even less intrusive than in *Tuggle*, where the Government surveilled a defendant for eighteen months with recorded video footage (which this Court found permissible). Nor does the limited CrimsonCard data accessed by IU rise to the level of the prohibited warrantless surveillance described in *Jones* (2,000 data points over 4 weeks) or *Carpenter* (13,000 data points over 4 months).

In view of the above, the limited CrimsonCard data IU accessed does not provide an "intimate window" into Appellants' lives, detailing their "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S.Ct at 2217 (citation and quotation omitted). Nor does it allow IU to "explore details of [Appellants' home(s)] that would previously have been unknowable without physical intrusion." *Kyllo*, 533 U.S. at 40. Rather, the CrimsonCard simply authenticates and then logs one's access (or rejected access) to IU's buildings and campus facilities, a record of which is then retained only for several months pursuant to normal records retention schedules. (*See* Dkt. 50 at 14) (noting that verification of a student's identity to confirm access is an express purpose of the CrimsonCard).

C. Appellants were not entitled to "precompliance" review before IU accessed its own institutional data.

Appellants' argument that the University must "obtain pre-compliance review" before accessing its own records is wrong, as is their analysis regarding the "subject" of the search. (*See* Appellants' Br. at 13-14) (citing *City of Los Angeles v. Patel*, 576 U.S. 409, 420 (2015)). The ordinance at issue in *Patel* required hotels to record detailed information about their guests and turn that information over to police on demand. *See Patel,* 576 U.S. at 413-14. "A hotel owner who refuse[d] to

give an officer access to his or her registry [could be] arrested on the spot." *Id.* at 421. And there is nothing in *Patel* that suggests the guests were entitled to pre-compliance review. Contrary to Appellants' argument, the hotel guests *were* the ultimate subjects of the police investigation; the ordinance provided access to the hotels' files on guests to combat crime. That's the entire point of the law.[9] Because the registration information at issue in *Patel* was the hotels' business records, the hotel would have been free to search its own registry.

In much the same way, since IU owns the CrimsonCard records at issue here, IU's search of its own records similarly does not require pre-compliance review. (*See supra* at 21-23) (explaining that cards are intended to be read by third-parties and necessarily communicate data through a cardholder's use of same). Again, contrary to Appellants' argument, the correct inquiry is "reasonableness." *See Naperville*, 900 F.3d at 528 (where searches "are not performed as part of a criminal investigation, [the Court] can turn immediately to an assessment of whether they are reasonable") (cleaned up); *Medlock,* 738 F.3d at 872 (for purposes of university housing inspections, the Fourth Amendment's warrant requirement "can be satisfied by demonstrating the reasonableness of the regulatory package … ") (quoting *Platteville Area Apartment Ass'n v. City of Platteville*, 179 F.3d 574, 578 (7th Cir. 1999)). The Court must "balance[e] [the] intrusion on the individual's Fourth

[9] *See Patel*, 576 U.S. at 428 (Scalia, J., dissenting) ("The purpose of this recordkeeping requirement is to deter criminal conduct, on the theory that criminals will be unwilling to carry on illicit activities in motel rooms if they must provide identifying information …").

Amendment interests against its promotion of legitimate government interests." *Naperville*, 900 F.3d at 528 (cleaned up).

In *Medlock,* this Court found no Fourth Amendment violation where University inspectors entered a student's dorm room for purposes of a health and safety inspection. In doing so, the Court noted that

> Medlock had consented in advance, as a condition of being allowed to live in the dormitory, to have his room searched for contraband and other evidence in violation of the health and safety code. He could have lived off campus and thus have avoided being governed by the code. *He chose to trade some privacy for a dorm room*. His expulsion amounted to holding him to his contract.

738 F.3d at 872 (emphasis added). Appellants, too, chose to trade some privacy for living in the University's residence halls, entry to which runs through the CrimsonCard. If the physical search of a dorm room for a health and safety inspection is not a Fourth Amendment violation, IU's limited review of CrimsonCard data relating to Appellants' residence hall access for the legitimate University purpose of investigating a hazing incident surely cannot be a violation, either.

Appellants' argument that *Medlock* is inapplicable because "this was not a routine health-and-safety inspection" is illogical. (Appellants' Br. at 9.) True, CrimsonCard data "cannot show whether you are respecting your roommate by maintaining a clean-living area," (*id.*), but it might reveal that a fraternity is subjecting its pledge class (comprised of predominantly freshman students living in University housing) to hazing tactics, such as schedule alteration, sleep deprivation,

or obstructing and endangering the academic process.[10] A university's mission to protect its students' well-being applies equally to ensuring their safety from hazards inside of their dorm room, as well as to hazards outside of it.

Appellants' claim that this case is also different than *Medlock* because the search was performed by a University official rather than an RA, (*see id.* at 9), is also unpersuasive. In fact, this Court expressly said the opposite, finding that "even if the student inspectors had been public officers, their search of Medlock's dorm room would have been a lawful regulatory search." *Medlock,* 738 F.3d at 872. For purposes of university housing inspections, the Fourth Amendment's warrant requirement "can be satisfied by demonstrating the reasonableness of the regulatory package … ." *Id.* (internal citations omitted).

Here, as set forth above, for purposes of the Fourth Amendment, Appellants did not have a reasonable expectation of privacy in the CrimsonCard data at issue. Even if they did, however, such an interest would be diminished for two important reasons. *First*, the CrimsonCard data was collected without prosecutorial intent toward Appellants, despite their attempt to now assert (without any basis in reality, nor was it alleged in their Complaint) that the University somehow intended to "convict [Appellants] of the administrative equivalent of perjury." (Appellants' Br. at 5.) *See Naperville*, 900 F.3d at 528 (limiting privacy interest where data was not collected by law enforcement and there was no risk of criminal prosecution) (citing

[10] *See* "Hazing Terms & Examples," INDIANA UNIVERSITY, DIVISION OF STUDENT AFFAIRS, available at: https://studentaffairs.indiana.edu/get-involved/student-organizations/manage-organization/policies/hazing-definitions.html (last visited Dec. 6, 2021).

Camara v. Mun. Court of City and County of San Francisco, 387 U.S. 523, 531 (1967)). Here, IU accessed the data only to confirm that *Appellants were not the victims of hazing*, not to impose any sort of discipline on them.[11]

Second, the data was collected without physical entry into Appellants' home(s). *Id.* (citing *Camara*'s concern that physical entry posed a "serious threat to personal and family security"). This limited privacy interest pales in comparison to IU's interest in investigating allegations of, and working to protect its students from, hazing, which is prohibited by both IU's Code of Student Rights, Responsibilities, and Conduct and by Indiana law, *see* Ind. Code § 35-42-2-2.5. To be clear, IU's investigation resulted in sanctions for Beta Theta Pi, but no adverse actions were considered, let alone taken, against Appellants. (Dkt. 1 at 4, ¶ 19.) As such, IU's actions in accessing limited CrimsonCard data for the legitimate purposes of investigating a complaint of hazing and promoting the safety of Appellants and the University community, were more than reasonable and did not require any pre-compliance review.

---

[11] Appellants' attempt to impart the disciplinary proceedings against their fraternity to themselves is an attempt to create alleged constitutional rights (or violations) where there are none. (*See, e.g.*, Appellants' Br. at 9-10.) Appellants' reliance on *Doe v. Baum,* 903 F.3d 575 (6th Cir. 2018), is especially flawed. (*See id.* at 10.) Not only did *Baum* involve an investigation into Title IX sexual misconduct (for which some courts have found that universities should offer heightened due process protections, and for which this Court has so far declined to address), but it was in the context of an *individual* conduct proceeding. Further, that *Baum* required the university to afford a student accused of sexual misconduct certain due process protections, including an opportunity for cross-examination at a hearing, is of no moment here. No conduct charges were ever brought against Appellants, and nothing suggests the fraternity wasn't afforded due process in connection with its disciplinary sanctions.

Thus, IU's review of the limited CrimsonCard data for the legitimate purpose of investigating a complaint of hazing (of which, as fraternity pledges, Appellants would have been victims, not perpetrators) (*see id.*), and working to protect the safety and well-being of its students—which is a legitimate and anticipated use of the CrimsonCard's data pursuant to IU's Management of Institutional Data Policy (DM-01)—was reasonable and did not violate the Fourth Amendment. *Jones,* 565 U.S. at 410 (citing *Karo,* 468 U.S. at 712); *see also generally Yost v. Wabash College,* 3 N.E.3d 509, 518 (Ind. 2014) (recognizing, in context of a negligence action, that "colleges and universities should be encouraged, not disincentivized, to undertake robust programs to discourage hazing …"). IU's interest in ensuring student safety and well-being, particularly given Appellants' status as freshmen living in on-campus University housing, when balanced against the relatively low-degree of intrusion, demonstrates the reasonableness of IU's access of the limited CrimsonCard data at issue. Indeed, as the district court found, IU's actions were "plainly legitimate." (Dkt. 50 at 15-16.) IU, therefore, respectfully requests that the Court affirm the district court's dismissal of Appellants' Complaint in its entirety.

CONCLUSION

The Judgment of the district court should be *affirmed* in all respects.

Respectfully submitted,

ICE MILLER LLP

/s/ Jenny R. Buchheit

Jenny R. Buchheit (counsel of record)
Sean T. Dewey
ICE MILLER LLP
One American Square, Suite 2900
Indianapolis, IN 46282-0200
(317) 236-2295 (telephone)
(317) 592-5487 (facsimile)
jenny.buchheit@icemiller.com
sean.dewey@icemiller.com

Attorneys for Appellees Indiana University, Bloomington, and Pamela S. Whitten, in her official capacity as President of Indiana University

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)(7)

Pursuant to Rule 32(a)(7) of the Federal Rules of Appellate Procedure, I hereby certify that this brief complies with the stated type-volume limitations. The text of this brief was prepared in Century Schoolbook 12-point font, with footnotes in Century Schoolbook 12-point font. All portions of the brief, other than the Disclosure Statements, Table of Contents, Table of Authorities, and the Certificates of Counsel, contain 8,802 words. This certification is based on the word count function of the Microsoft Office Word word processing software, which was used in preparing this brief.

Dated: December 8, 2021 /s/ Jenny R. Buchheit

CERTIFICATE OF SERVICE

I hereby certify that on December 8, 2021, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Jenny R. Buchheit

4886-4972-5700