No. 130337

In the Supreme Court of Illinois

REBECCA PETTA on her own behalf and on behalf of those similarly situated,	)	On Appeal from the Appellate Court of Illinois, Fifth Judicial District, Case No. 5-22-0742
Plaintiff-Appellant	)	
v.	)	Appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, No. 22-LA-51
CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRISTIE CLINIC,	)	The Honorable Jason M. Bohm, Judge Presiding
Defendant-Appellee.	)	

AMICI CURIAE BRIEF OF THE ILLINOIS HEALTH AND HOSPITAL ASSOCIATION AND THE ILLINOIS STATE MEDICAL SOCIETY

Hugh C. Griffin (ARDC# 1058770) (*hgriffin@hpslaw.com)*
HALL PRANGLE & SCHOONVELD, LLC
200 South Wacker Drive, Suite 3300
Chicago, Illinois 60606
Phone: (312) 267-6234 / Fax: (312) 345-9608
Firm ID No. 39268
Email service: *HPSDocket@hpslaw.com*
Attorney for Amici Curiae, The Illinois Health and Hospital Association and *The Illinois State Medical Society*

E-FILED
8/26/2024 3:19 PM
CYNTHIA A. GRANT
SUPREME COURT CLERK

No. 130337

In the Supreme Court of Illinois

REBECCA PETTA on her own behalf and on behalf of those similarly situated,	)	On Appeal from the Appellate Court of Illinois, Fifth Judicial District, Case No. 5-22-0742
Plaintiff-Appellant	)	
v.	)	Appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, No. 22-LA-51
CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRISTIE CLINIC,	)	The Honorable Jason M. Bohm, Judge Presiding
Defendant-Appellee.	)	

AMICI CURIAE BRIEF OF THE ILLINOIS HEALTH AND HOSPITAL ASSOCIATION AND THE ILLINOIS STATE MEDICAL SOCIETY

TABLE OF CONTENTS AND STATEMENT OF POINTS AND AUTHORITIES

STATEMENT OF INTEREST OF AMICI CURIAE

The Illinois Health and Hospital Association ("IHA") is a state-wide, not-for-profit organization. IHA's purpose is to ensure that all individuals and communities have access to high-quality health care at the right time and in the right setting. IHA represents over 200 Illinois hospitals and nearly 40 Illinois health care systems. For over 80 years, IHA has served as a representative and advocate for its members, addressing the social, economic, political, and legal issues affecting the delivery of high-quality health care in Illinois.

Unfortunately, criminal cyberattacks, like that which occurred here, have also been made against members of the IHA.[1] Like Christie Clinic, IHA members must of necessity keep personal identity and health information of their patients on their computer systems in order to provide appropriate health care to those patients. Thus, IHA's membership has a profound interest in both the standing and substantive issues presented by this appeal.

The Illinois State Medical Society ("ISMS") is comprised of thousands of participating physicians, residents, and medical students, including pediatric specialists. ISMS's mission is to promote the science and art of medicine, the protection of public health and the betterment of the medical profession. ISMS also

---

[1] See "800,000 people's data stolen in Lurie Children's Hospital cyberattack," *Chicago Sun Times* (online), July 2, 2024 (A 1-2); "Patient data likely stolen in Ascension cyberattack: Health care system says perpetrators took files from 7 of 25,000 servers," *Chicago Tribune*, June 14, 2024, Business Sec., p. 1. (A 3-4); "Information of 10,300 people may have been exposed in University of Chicago Medical Center email incident," *Chicago Tribune* (online), May 29, 2024. (A 5-6).

has a profound interest in this case because many of its members practice in clinics or practice groups like Christie Clinic, and thus, they are also potential targets of criminal cyberattacks.

Mindful that it is a privilege and not a right to appear as an amicus curiae before this Court, IHA and ISMS are grateful for the opportunity to do so in this case. IHA and ISMS respectfully submit that they can bring to the Court an analysis and front-line perspective of their membership that will assist the Court in properly deciding the issues before it.

ARGUMENT

I. The Appellate Court Correctly Held that Plaintiff Lacked Standing to Bring the Instant Action.

The appellate court correctly ruled that Illinois standing law requires more than a speculative "increased risk of harm" (Opinion ¶ 16), which is ultimately all that plaintiff pled even with the assertion that publicly available information – *i.e.,* her phone number and address but not her name – were used in an unauthorized loan application. (Opinion ¶ 20). Accord, *Maglio v. Advocate Health and Hosps. Corp.*, 2015 IL App (2d) 140782, ¶¶ 24-30. Furthermore, as the appellate court concluded, those allegations were also insufficient to establish another standing requirement, *i.e.,* that the alleged suspicious behavior was "fairly traceable" to the alleged data breach at issue:

> "Anyone could have committed the fraud using the same readily available public information. There is no way, outside of speculating, for this court to determine that, had these hackers not breached the defendant's e-mail, Petta's phone

> number and address would still have not have been used fraudulently. The information would still have been public had this breach not occurred. Thus, we cannot trace the fraudulent activity back to the defendant's actions." (Opinion ¶ 23).

While some federal cases may have applied a more liberal view of standing (Opinion ¶ 16), the U.S. Supreme Court in *TransUnion, v. Ramirez*, 594 U.S. 413 (2021), clarified that standing in federal court requires plaintiffs to demonstrate that "they suffered a concrete harm," *id.* at 417, and that "an asserted *risk of future harm*" is not sufficient, *id.* at 435, "unless the exposure to the risk of future harm itself causes a *separate* concrete harm. *Id.* at 436 (all emphasis in original). Here, plaintiff alleges no "separate concrete harm."[2] Nor is this a case like *Flores v. Aon Corp.*, 2023 IL App (1st) 230140, ¶ 7 (Pl. Br. 14, 16, 23, 26-27). There, the court found standing based upon plaintiffs' ability to demonstrate actual fraudulent attempts to process a $499.99 payment on one plaintiff's PayPal account and an unauthorized prescription charge on another plaintiff's Express Scripts account. (*Id.*, ¶¶ 22-25). Nothing like that is alleged here. Thus, this Court should not even reach the substantive issues discussed below.

---

[2] Studies have shown that most data breaches do not result in any actual account fraud. See *In Re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (citing a GOA report).

II. Plaintiff Has Not Pled a Cognizable Cause of Action under Illinois Common Law or Statutory Law.

A. Christie Clinic had no common law duty to safeguard plaintiff's information.

In *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358 (1st Dist. 2010), where defendant accidentally disclosed personal information about 1700 former employees including social security numbers and personal health insurance information, the appellate court soundly held that:

> "While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review. As noted, the legislature has specifically addressed the issue and only required the Board to provide notice of the disclosure." *Id.* at 363.

The "legislative requirements already in place" referenced by the *Cooney* court are found in the Personal Information Protection Act ("PIPA"), 815 ILCS 530/1 *et seq.*, which then provided that in the event of such a data breach, the data collector "shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." 815 ILCS 530/10(b) (West 2006); *Cooney*, 407 Ill. App. 3d at 362.

Plaintiff points to the fact that seven years subsequent to the decision in *Cooney*, PIPA was amended to add a provision that an Illinois data collector of records containing personal information of an Illinois resident "shall implement and maintain reasonable security measures to protect those records from unauthorized

access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45(a) (West 2017) (Pl. Br. 37). Plaintiff's argument proves too much and ignores the fact that the legislature, presumed to be aware of the decision in *Cooney*, *Nelson v. Artley*, 2015 IL 118058, ¶ 23, kept the remedy the same, *i.e.*, notification. The 2017 amendment broadened the notification requirements to include notice to the Attorney General, but did not provide for any private right of action or add any further remedy for an alleged violation of its provisions. 815 ILCS 530/10(e)(2). Thus, courts have followed the *Cooney* analysis even after the 2017 amendments to PIPA. See *e.g.*, *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760 (C.D. Ill. 2020); *In re SuperValu, Inc.*, 925 F.3d 955, 964 (8th Cir. 2019); *Toretto v. Donnelley Financial Solutions, Inc.*, 583 F. Supp. 3d 570, 591-92 (S.D.N.Y. 2022).

Amici acknowledge that one appellate court has reached a different result. See *Flores*, 2023 IL App (1st) 230140, ¶¶ 22-25, rejecting *Cooney* based solely on the PIPA amendment, without any express consideration of the fact that even after the amendment, the only remedy prescribed by the legislature was notice to those whose personal information may have been accessed and now also to the Attorney General. The *Flores* court's decision was also seemingly influenced by the fact that the defendant in that case (Aon) "is a sophisticated company that provides cyber security services to its clients, so it is well aware of the risks of providing inadequate security measures for personal information" and that "[p]roviding reasonable security measures for the storage of personal information would not be a large burden for defendant, given its experience and expertise in cyber security." *Id.* ¶ 24.

Here, defendant is a medical clinic whose expertise – like that of all medical clinics, hospitals and health care systems, and other medical care providers – is providing medical care, treatment, and services to its patients, not "provid[ing] cyber security services to its clients." Thus, *Flores* is not persuasive here.

B. There is no basis to judicially imply a separate private right of action for an alleged PIPA violation.

While there are instances where a private right of action has been judicially implied for violation of a statute that otherwise does not expressly provide for such a remedy, the requirements are strict, and each much be satisfied, including the requirement that "implying a private right of action is necessary to provide an adequate remedy for violations of the statute." *Fisher v. Lexington Health Care, Inc.*, 188 Ill. 2d 455, 460 (1999); *Metzger v. DaRosa*, 209 Ill. 2d 30, 36 (2004). Citing *Abbasi v. Paraskevoulakos*, 187 Ill. 2d 386, 395 (1999), this Court stated that under this "necessity" requirement, implication of a private right of action is appropriate "only in cases where the statute would be ineffective, as a practical matter, unless such an action were implied," *Fisher*, 188 Ill. 2d at 50-51, or where "the statutory framework . . . is so deficient that it is necessary to imply a private right of action . . . to effectuate its purpose." *Metzger*, 209 Ill. 2d at 42.

This "necessity" requirement is absent here for two reasons. *First*, all defendants subject to the risk of a criminal cyberattack, particularly medical clinics, hospitals and health care systems, and other medical care providers, are strongly motivated "to effectuate" PIPA's purpose and comply with PIPA's requirement to

"implement and maintain reasonable security measures to protect [its] records from unauthorized access" – given the severe impact that such an attack has on their ability to continue normal operations and provide necessary care and treatment to their patients.[3] *Second*, as set forth further below, the Consumer Fraud Act (CFA) provides a remedy for a PIPA violation to those plaintiffs who can demonstrate an actual economic loss. 815 ILCS 505/10(a).

C. Plaintiff has not alleged an actual economic loss necessary to assert a cause of action for a PIPA violation under the Consumer Fraud Act.

To the extent that the 2017 Amendment to PIPA has any effect on available causes of action for a data breach, it would be an action under the CFA. PIPA expressly provides that a violation of PIPA "constitutes an unlawful practice" under the CFA, 815 ILCS 530/20. However, to recover under the CFA, plaintiff must show an actual economic loss. 815 ILCS 505/10(a). The CFA requires proof of "actual damages in the form of specific economic injuries." *Morris v. Harvey Cycle and Camper, Inc.*, 392 Ill. App. 3d 399, 402 (1st. Dist. 2009). Accord *White v. DaimlerChrysler Corp.*, 368 Ill. App. 3d 278, 287 (1st Dist. 2006).

No such "actual damages in the form of specific economic injuries" is pled here. Indeed, the *Flores* court decided this issue correctly, rejecting plaintiffs' attempt to state a cause of action under the CFA for a violation of PIPA because

---

[3] It took Lurie Children's Hospital, the Ascension Hospital System, and University of Chicago Hospitals (all IHA members) many weeks to fully recover from the recent cyberattacks against them. (A 1-6).

plaintiffs failed to allege "an actual economic injury under the Consumer Fraud Act." *Flores*, 2023 IL App (1st) 230140, ¶ 40. Even though the *Flores* plaintiffs were able to allege attempts to charge their accounts for specific monetary amounts, that still did not constitute "the specific economic damages required for a claim under the Consumer Fraud Act." *Id.* at ¶ 42. Nor were allegations of emotional distress, lost time dealing with the consequences of the data breach, an increase in spam messages, and the imminent risk of fraud and identity theft sufficient to do so. *Id.* Here, plaintiff's assertion that her phone number and address were used in an unauthorized loan application does not come close even to the insufficient allegations in *Flores*; thus, plaintiff has not pled an "actual economic injury" required for a cause of action under the CFA.

D. The economic loss doctrine further bars plaintiff's negligence claim.

There is still one more reason to bar plaintiff's common law negligence claim. In *Moorman Mfg. Co. v. National Tank Co.*, 91 Ill. 2d 69, 81-86 (1982), this Court adopted the economic loss doctrine. "The economic loss rule bars a plaintiff from recovering for purely economic losses under a tort theory of negligence." *In Re Michaels Stores Pin Pad Litigation*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011), citing *Moorman*. Such losses are more appropriately addressed under contract law. *Id.; Moorman*, 91 Ill. 2d at 81. Accord *In Re Illinois Bell Switching Station Litigation*, 161 Ill. 2d 233, 240-41 (1994). The rule has three exceptions – (1) "where plaintiff sustains personal injury or property damage resulting from a sudden or

dangerous occurrence; (2) where plaintiff's damages were proximately caused by defendant's intentional, false representation; and (3) where plaintiff's damages were proximately caused by the negligent misrepresentation of a defendant in the business of supplying information for the guidance of others in business transactions." *In Re Michaels*, 830 F. Supp. 2d at 528, citing *Moorman*. As the circuit court soundly ruled, none of these exceptions are present here. (C 442-443 V2).

Furthermore, plaintiff's attempt to characterize her cause of action against Christie Clinic as independent of any contractual relationship between Christie Clinic and its patients fails on its face. Plaintiff asserts that her claim is "wholly outside of any agreed-upon medical services that Christie provided to Petta" (Pl. Br. 41-42), but then acknowledges that "Petta has a direct relationship with Christie as its patient" and Christie Clinic's obtaining, collecting, and storing Petta's personal and medical information was "[a]s a result of [Petta's] receiving medical services from Christie." (Pl. Br. 44). Plaintiff's second statement is correct. Christie Clinic, like all medical clinics, hospitals and health care systems, and other medical care providers, must of necessity keep personal health information and personal identity information of their patients on their computer systems in order to provide the "agreed-upon medical services" and appropriate health care to those patients.

Citing *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 418 (2004), plaintiff acknowledges that the "risk of unbounded liability" is another basis to bar tort claims under the economic damages rule. (Pl. Br. 43). This concern is especially

valid not only for Christie Clinic, but for all the other Illinois medical clinics, Illinois hospitals and health care systems, and other Illinois health care providers, given Illinois' recognized policy of "reduc[ing] the burden of litigation against health care professionals." *Kirk v. Michael Reese Hosp. and Med. Ctr.,* 117 Ill. 2d 507, 532 (1987). Here, permitting potentially hundreds of thousands of common law tort actions to proceed against Illinois medical clinics, hospitals and health care systems, and other health care providers would place an "unreasonable burden" on them when they too are the "victims" of a criminal cyberattack.

Plaintiff then asserts, without citing any authority, that a defendant's liability risk for a data breach is "fully insurable." (Pl. Br. 44). While we know of no Illinois authority holding that the existence or non-existence of a common law cause of action is determined on the basis of insurance availability, plaintiff's premise is faulty. Cyber insurance policies can have many provisions that can limit or even bar coverage. See "Cyber Insurance Exclusions: Are You Covered?" https://www.pondurance.com/blog/cyber-insurance-exclusions/#:~:text=Cyber%20insurance%20coverage%20exclusions%20in,acts%20of%20war%2C%20and%20more (last visited 8/8/24). (A 7-9).

CONCLUSION

For the reasons set forth herein and in the Appellee's Brief, the Illinois Health and Hospital Association and The Illinois State Medical Society respectfully request that the appellate court's decision be affirmed.

Respectfully submitted,

THE ILLINOIS HEALTH AND
HOSPITAL ASSOCIATION and
THE ILLINOIS STATE MEDICAL SOCIETY

By: */s/ Hugh C. Griffin*
Hugh C. Griffin, their attorney

Hugh C. Griffin (ARDC# 1058770) (*hgriffin@hpslaw.com)*
HALL PRANGLE & SCHOONVELD, LLC
200 South Wacker Drive, Suite 3300
Chicago, Illinois 60606
Phone: (312) 267-6234 / Fax: (312) 345-9608
Firm ID No. 39268
Email service: *HPSDocket@hpslaw.com*
Attorney for Amici Curiae, The Illinois Health and Hospital Association and *The Illinois State Medical Society*

Supreme Court Rule 341(c) Certification of Compliance

Pursuant to Supreme Court Rule 341(c), I certify that this Amici Curiae's Brief conforms to the requirements of Rules 341(a), (b) and Rule 345. The length of this brief, excluding the pages containing the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service and the matters contained in the Appendix, is **11** pages.

Respectfully submitted,

THE ILLINOIS HEALTH AND
HOSPITAL ASSOCIATION and
THE ILLINOIS STATE MEDICAL SOCIETY

By: */s/ Hugh C. Griffin*
Hugh C. Griffin, their attorney

Hugh C. Griffin (ARDC# 1058770) (*hgriffin@hpslaw.com)*
HALL PRANGLE & SCHOONVELD, LLC
200 South Wacker Drive, Suite 3300
Chicago, Illinois 60606
Phone: (312) 267-6234 / Fax: (312) 345-9608
Firm ID No. 39268
Email service: *HPSDocket@hpslaw.com*
Attorney for Amici Curiae, The Illinois Health and Hospital Association and *The Illinois State Medical Society*

APPENDIX

APPENDIX

TABLE OF CONTENTS

CS★T

800,000 people's data stolen in Lurie Children's Hospital cyberattack

By Emmanuel Camarillo
Jul 2, 2024, 7:02pm CDT

The personal data of nearly 800,000 people was leaked during a months-long cyberattack at Lurie Children's Hospital this year that forced the institution to shut down its entire network.

The hospital said 791,784 people were affected by the hack, which investigators determined began in late January, according to a data breach notice filed last week with the Office of the Maine Attorney General.

Personal data that was leaked included Social Security numbers, medical conditions or diagnoses, addresses, driver's license numbers and prescription information, the hospital said in a notice on its website.

Cybercriminals accessed Lurie's system's between Jan. 26 and Jan. 31, the hospital said. Phone, email and electronic systems were taken offline on Jan. 31 in response to the attack, though the hospital remained open throughout the outage.

MyChart, the hospital's patient portal, was also shut down, leaving some parents frustrated with the response times of the call center that was established after the network was shut down.

The hospital slowly reestablished its network over the next several weeks. Emails and phone lines went back online by mid-February. And its electronic medical records platform was restored in early March. But it wasn't until May 20 that the hospital said it was no longer combating the cybersecurity threat.

The hospital said it did not pay a ransom and instead worked with law enforcement to retrieve data once investigators determined how much had been affected by the attack.

The Rhysida ransomware group was allegedly behind the attack, according to cybersecurity news outlet The Record, which also said the group made more than $3 million from selling the data it stole.

The hospital said it is notifying individuals whose data was stolen, including through mailing notification letters. "Our notification material will identify resources to help protect their identity."

Cybercriminals have targeted at least two other hospital systems in the Chicago area this year.

In May, a ransomware attack forced hospital group Ascension's computer systems offline and diverted ambulances away from some of its emergency departments, including one in the Chicago area.

The same month, University of Chicago Medical Center said it was a victim of a hack that may have exposed patient data.

"Hospitals and health systems across the country face constantly evolving cybersecurity threats," Lurie Children's said. "For our part, we are working closely with our internal and external experts to further enhance the security of our systems.

The hospital has established a call center for anyone who may have questions about the attack and the hospital's response. The call center can be reached at (888) 401-0575 between 8 a.m. and 8 p.m. Monday through Friday.

Patient data likely stolen in Ascension cyberattack: Health care system says perpetrators took files from 7 of 25,000 servers

Schencker, Lisa

FULL TEXT

Cybercriminals stole files from hospital system Ascension that likely contained personal information, Ascension said in a statement Wednesday, about a month after revealing it had fallen victim to a ransomware attack.

Ascension said it now has evidence that the attackers took files from seven of the system's 25,000 file servers.

Ascension is still investigating but said it believes those files may contain protected health information and personally identifiable information for some individuals. The system does not yet know exactly which data was stolen or from which patients, Ascension said.

Ascension said it has no evidence that the attackers stole data from its electronic health records. The system said the attack occurred after a person working at one of its facilities accidentally downloaded a malicious file that the person thought was legitimate.

Ascension is offering free credit monitoring and identity theft protection services to any patient or employee who would like the services, and those who wish to enroll can call 1-888-498-8066.

Ascension is a nationwide health system with about 150 sites of care in Illinois, including 14 hospitals.

The system has said that it discovered the attack on May 8. The systems' hospitals and clinics postponed some elective surgeries and appointments, and one Ascension Illinois hospital temporarily went on ambulance bypass, meaning ambulances were asked to take new patients to other hospitals.

A nurse in at least one of Ascension's Illinois hospitals said, shortly after the attack, nurses couldn't automatically see doctors' orders for patients, such as for medication or tests, or use their usual procedures to ensure accuracy when administering medication to patients.

Ascension Illinois said earlier this week that it had restored the primary technology it uses for electronic patient documentation, which would allow hospitals and doctors offices to again document, chart and send orders electronically.

The incident at Ascension was one of the latest in a string of cyberattacks on health care institutions in Illinois and across the country. Lurie Children's Hospital in Chicago was attacked in January, and University of Chicago Medical Center said in late May that the information of about 10,300 people may have been exposed in a phishing incident.

Cybercriminals often target health systems because of their size, their dependence on technology and the large amounts of sensitive data they hold, according to the U.S. Department of Health and Human Services.

CREDIT: By Lisa Schencker Chicago Tribune

DETAILS

Subject:	Hospitals; Patients
Business indexing term:	Subject: Hospitals

A 3

Location:	Chicago Illinois; United States--US; Illinois
Publication title:	Chicago Tribune; Chicago, Ill.
First page:	1
Publication year:	2024
Publication date:	Jun 14, 2024
Section:	Business
Publisher:	Tribune Publishing Company, LLC
Place of publication:	Chicago, Ill.
Country of publication:	United States, Chicago, Ill.
Publication subject:	General Interest Periodicals--United States
ISSN:	10856706
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	3067763973
Document URL:	https://proxy.cc.uic.edu/login?url=https://www.proquest.com/newspapers/patient-data-likely-stolen-ascension-cyberattack/docview/3067763973/se-2?accountid=14552
Copyright:	Copyright Tribune Publishing Company, LLC Jun 14, 2024
Last updated:	2024-06-14
Database:	Chicago Tribune

LINKS

Linking Service

Information of 10,300 people may have been exposed in University of Chicago Medical Center email incident

Schencker, Lisa

FULL TEXT

A phishing incident involving the emails of workers at University of Chicago Medical Center may have exposed the personal information of about 10,300 people, according to the hospital.

The email accounts of several hospital workers were accessed between Jan. 4 and Jan. 30, the hospital said in a news release. When the hospital learned of the incident, it took steps to secure those email accounts, and it launched an investigation.

In late March, the hospital determined that the email accounts contained health information, and for some people may have also included Social Security numbers, passport numbers, driver's license numbers, insurance information, billing information and access information, such as security questions and answers.

"UCMC remains committed to protecting the confidentiality of all faculty, staff, students and patients and takes cybersecurity threats to its systems seriously," the hospital said in a news release. "It has taken steps to prevent a similar occurrence from happening again, including implementation of additional technical safeguards."

Phishing is when cybercriminals attempt to access sensitive data through fraudulent emails or websites, according to the National Institute of Standards and Technology.

Affected individuals may call 833-918-4065 Monday through Friday from 8 a.m. to 8 p.m. with questions.

The security incident follows a string of high-profile cyberattacks on health care institutions in the Chicago area and across the country. Earlier this month Ascension, which has 14 hospitals in Illinois, said it was the victim of a ransomware attack. The attack led Ascension to postpone some nonemergency elective surgeries, tests and appointments and temporarily divert ambulances carrying new patients from one Illinois hospital.

In January, Lurie Children's Hospital in Chicago also faced a cyberattack. It took more than a month for Lurie to get all of its systems back online after the attack.

Health care institutions are often targets for cybercriminals because of their size, their dependence on technology and the large amounts of sensitive data they hold, according to the U.S. Department of Health and Human Services.

DETAILS

Subject:	Electronic mail systems; Cybercrime
Location:	Chicago Illinois; United States--US; Illinois
Company / organization:	Name: University of Chicago Medical Center; NAICS: 622110
Publication title:	Chicago Tribune (Online); Chicago

Publication date:	May 29, 2024
Publisher:	Tribune Publishing Company, LLC
Place of publication:	Chicago
Country of publication:	United States, Chicago
Publication subject:	General Interest Periodicals--United States
Source type:	Blog, Podcast, or Website
Language of publication:	English
Document type:	News
Publication history :	
Milestone dates:	2024-05-29 (Modified)
ProQuest document ID:	3061480638
Document URL:	https://proxy.cc.uic.edu/login?url=https://www.proquest.com/blogs-podcasts-websites/information-10-300-people-may-have-been-exposed/docview/3061480638/se-2?accountid=14552
Copyright:	Copyright Tribune Publishing Company, LLC 2024
Last updated:	2024-06-01
Database:	Chicago Tribune

LINKS

Linking Service

PONDURANCE

Cyber Insurance Exclusions: Are You Covered?

https://www.pondurance.com/blog/cyber-insurance-exclusions/#:~:text=Cyber%20insurance%20coverage%20exclusions%20in,acts%20of%20war%2C%20and%20more.

Pondurance
December 07, 2023

Year after year, cyberattacks just keep coming. Today, ransomware is the primary threat from cybercriminals, particularly in the healthcare, government facilities, and critical manufacturing industries. The average ransom payment nearly doubled from $812,000 in 2022 to over $1.54 million in 2023, according to Sophos' report *The State of Ransomware 2023*. In addition to the ransom payment, the average cost to recover from a ransomware attack is $1.82 million.

As a result of the escalating costs of an attack, insurers have increased premiums over the years and are now imposing stricter requirements to qualify for a policy. With so much at risk, it's more important than ever to understand what your cyber policy covers — and what it doesn't cover, known as exclusions.

Cyber insurance coverage exclusions in an insurance policy can include failure to maintain standards, payment card industry (PCI) fines and assessments, prior acts, acts of war, and more.

FAILURE TO MAINTAIN STANDARDS

Your company should have procedures and controls in place to protect against cyberattacks, and insurers want to know these protections are at work. Upon application, all insurers require that you answer fundamental questions about your cyber risks to get accepted for a cyber insurance policy. Once accepted, a "failure to maintain standards" exclusion allows the insurer to deny claims if your company doesn't keep up with adequate security standards or follow best practices during the coverage period.

The language of the exclusion varies widely. You should ask an insurer to remove any ambiguous language in a cyber insurance policy to assure that the standards are clear. Does the insurer require that you use multifactor authentication to protect specific accounts? Is there a timeline for making patches? Does the insurer require periodic phishing training for employees during the policy period? Knowing the answers to these questions and others can ensure that you won't be denied coverage following a cyberattack or breach.

"Companies with cyber insurance must fully understand what they need to do to maintain the provisions of a policy," said Doug Howard, CEO at Pondurance. "The first step is making sure there's no ambiguity in the language of the required standards. Then, during the coverage period, stay diligent about complying with those standards to minimize your vulnerabilities and maintain your coverage in case you need to file a claim."

PCI FINES AND PENALTIES

After a breach, fines and penalties can be assessed against your company from payment cards, such as Visa and Mastercard — and the fines can be costly. Most insurers will put some restrictions on coverage, so it's necessary to carefully review your policy for adequate limits and deductibles. If your company is subject to PCI fines or penalties and the exclusion applies, it can be a hefty loss for your business.

As a real-world example, a national restaurant chain experienced a data breach where cybercriminals obtained 60,000 customer credit card numbers and posted them on the internet. Mastercard imposed three assessments on the restaurant chain's credit card processor: $1.7 million for fraud recovery, $163,123 for operational reimbursement, and $50,000 for a case management fee. The restaurant chain paid the assessments and made a claim to the insurer, but the insurer denied coverage. The restaurant chain filed a lawsuit, and the court dismissed all claims based on the language of the exclusions. The restaurant chain didn't receive coverage for any of the assessment amounts.

"A cyber insurance claim that falls within this exclusion can be an unexpected hit to the bottom line, especially for small and midsize businesses," said Doug. "It's important to carefully consider any exclusions and requirements, line by line, the required assessments both by the cyber carrier and for any regulatory bodies applicable to you (state, industry, federal) and the entirety of the language in your cyber policy."

PRIOR ACTS

A prior acts exclusion prevents a claim for activity that happened before the retroactive date or the first date of a policy. This exclusion can be especially significant in a cyber insurance policy because breaches aren't always detected until long after they first occur. In fact, the average time to detect and contain a breach is 277 days, according to IBM Security's *Cost of a Data Breach Report 2023*.

Your company should take proactive steps to make sure your cyber insurance policy covers any possible breach. For example, when changing insurers, you may want to buy an extended discovery period that offers additional coverage for claims that might have initially happened under the previous policy. Or you may want to choose a retroactive date that precedes the start of the new policy.

ACTS OF WAR

War, terrorism, and insurrection typically fall under an act of war exclusion in a traditional insurance policy. However, a cyber insurance claim can involve nation-states, or cyber activity attributed to a suspected nation-state, where hostile attacks are made on U.S.-based companies and data and business operations are held hostage in exchange for large payouts. But, is that an act of war?

The New Jersey courts recently decided an acts of war exclusion lawsuit. The case involved the 2017 Russian cyberattack on Ukraine, known as the NotPetya attack, that impacted U.S. businesses including pharmaceutical giant Merck & Co. Merck claimed it incurred $1.4 billion in damages and filed a claim with its insurer. The insurer denied coverage based on the acts of war exclusion, so Merck sued. In January 2022, the judge ruled that the insurer can't claim the acts of war exclusion because the language in the policy applies to traditional forms of warfare, not a cyberattack. In 2023, the New Jersey appellate court affirmed the lower court decision. The insurer must pay the claim to Merck. As a result, insurers will likely revise the language in their policies to include nontraditional forms of warfare.

"Requirements and exclusions aren't always onerous, rather they're something you just need to understand when you're agreeing to a contract. The courts have weighed in on some exclusion clauses in cyber policies, particularly the acts of war clause, although not always consistently between cases, and they don't always rule on the side of the policyholder," said Doug. "That's why you need to comb through each line of the exclusion language to know exactly what your policy covers and do not assume that the exclusion will never apply to your organization. Legal advice is always recommended."

CONCLUSION

Cyberattacks continue to occur, and the price for a ransomware attack or data breach can be quite costly. Pay close attention to the exclusions when negotiating your cyber insurance policy to ensure that you won't suffer greater losses than expected when filing a claim.

Don't want to go at it alone? Working with a managed detection and response provider can help you maintain cybersecurity standards that cyber insurers require and be your partner in case of an incident.

No. 130337

In the Supreme Court of Illinois

REBECCA PETTA on her own behalf and on behalf of those similarly situated, Plaintiff-Appellant v. CHRISTIE BUSINESS HOLDINGS COMPANY, P.C. d/b/a CHRISTIE CLINIC, Defendant-Appellee.	)	On Appeal from the Appellate Court of Illinois, Fifth Judicial District, Case No. 5-22-0742 Appeal from the Circuit Court of Champaign County, Illinois, Sixth Judicial Circuit, No. 22-LA-51 The Honorable Jason M. Bohm, Judge Presiding

NOTICE OF FILING and CERTIFICATE OF SERVICE

TO: See Attached Service List

You are hereby notified that on **August 15, 2024**, we electronically submitted to the Clerk of the Supreme Court of Illinois, through eFileIL, ***Amici Curiae Brief of The Illinois Health and Hospital Association and The Illinois State Medical Society,*** and ***Notice of Filing and Certificate of Service***, true and correct copies of which are attached and hereby served upon you.

Respectfully submitted,

THE ILLINOIS HEALTH AND HOSPITAL ASSOCIATION and THE ILLINOIS STATE MEDICAL SOCIETY

By: */s/ Hugh C. Griffin*
Hugh C. Griffin, their attorney

Hugh C. Griffin (ARDC# 1058770) (*hgriffin@hpslaw.com)*
HALL PRANGLE & SCHOONVELD, LLC
200 South Wacker Drive, Suite 3300
Chicago, Illinois 60606
Phone: (312) 267-6234 / Fax: (312) 345-9608
Firm ID No. 39268
Email service: *HPSDocket@hpslaw.com*
Attorney for Amici Curiae, The Illinois Health and Hospital Association and *The Illinois State Medical Society*

CERTIFICATE OF SERVICE

I, the undersigned, a non-attorney, certify that on **August 15, 2024**, true and correct copies of the attached ***Amici Curiae Brief of The Illinois Health and Hospital Association and The Illinois State Medical Society,*** and ***Notice of Filing and Certificate of Service***, were electronically submitted and served via eFileIL and e-mail to the attorneys of record on the attached Service List.

Under penalties as provided by law pursuant to Section 1-109 of the Illinois Code of Civil Procedure, I certify that the statements set forth in this instrument are true and correct to the best of my knowledge, information, and belief.

By: */s/ Denise L. Smith*
Denise L. Smith

SERVICE LIST

David M. Cialkowski
Brian C. Gudmundson
Michael J. Laird
Rachel K. Tack
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Phone: (612) 341-0400
david.cialkowski@zimmreed.com
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings
THE JOHNSON FIRM
610 President Clinton Avenue, Suite 300
Little Rock, AR 72201
Phone: (501) 372-1300
cjennings@yourattorney.com

Attorneys for Plaintiff-Appellant Rebecca Petta

Jonathan B. Amarilio
Jeffrey M. Schieber
Jaimin Shah
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker Drive, Suite 2600
Chicago, IL 60601
Phone: (312) 527-4000
jamarilio@taftlaw.com
jschieber@taftlaw.com
jshah@taftlaw.com

Attorneys for Defendant-Appellee Christie Business Holdings Company, P.C. d/b/a Christie Clinic