Cyber Incidents: Maximizing Recoveries, Minimizing Legal and Regulatory Risks, Preserving Stakeholder Trust

November 19, 2024

ACC Association of Corporate Counsel CHICAGO

CRA Charles River Associates

Roundtable Leaders

Kris Swanson
Charles River Associates

Daniel Healy
Brown Rudnick

Jordan Kraner
Charles River Associates

Anne Reader
TransUnion

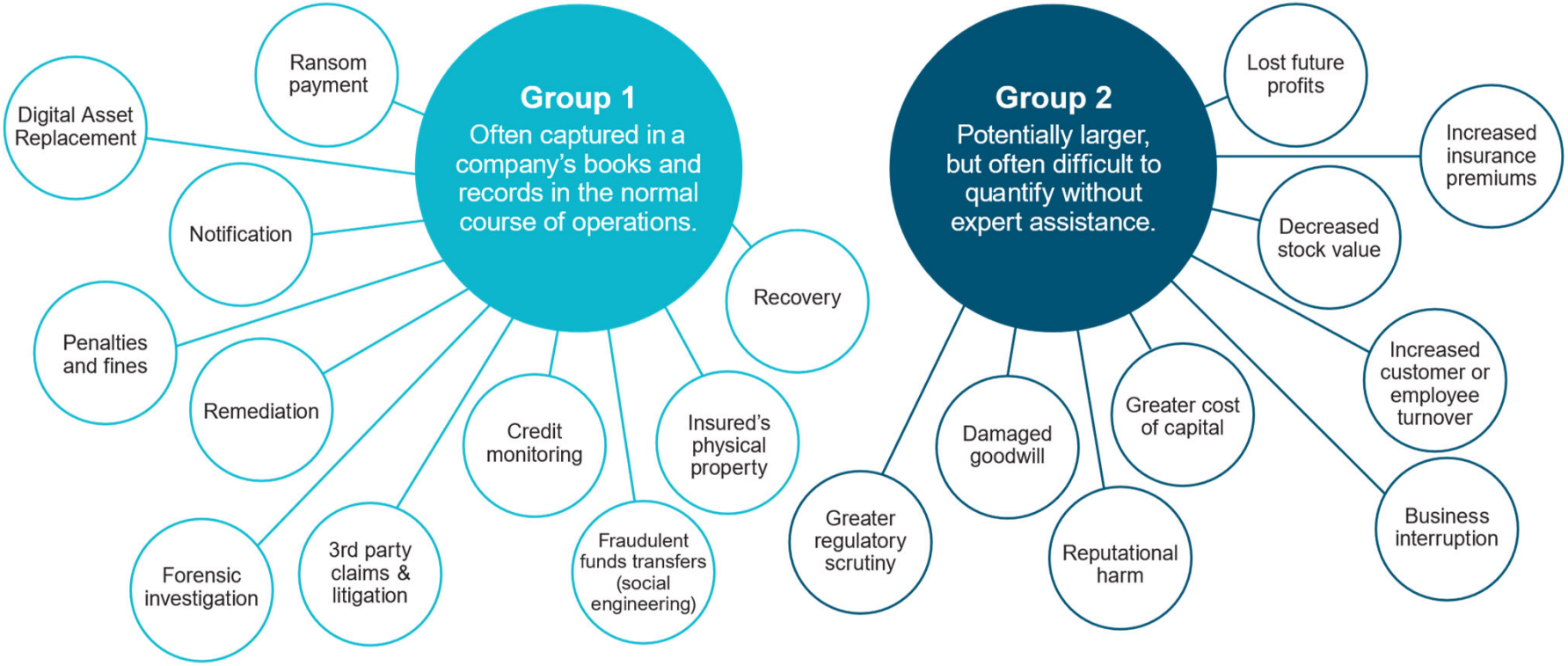
Kevin Small
Hunton Andrews Kurth

Jim Tu
McDonalds

CRA Charles River Associates

What cyber costs and damages can you recover?

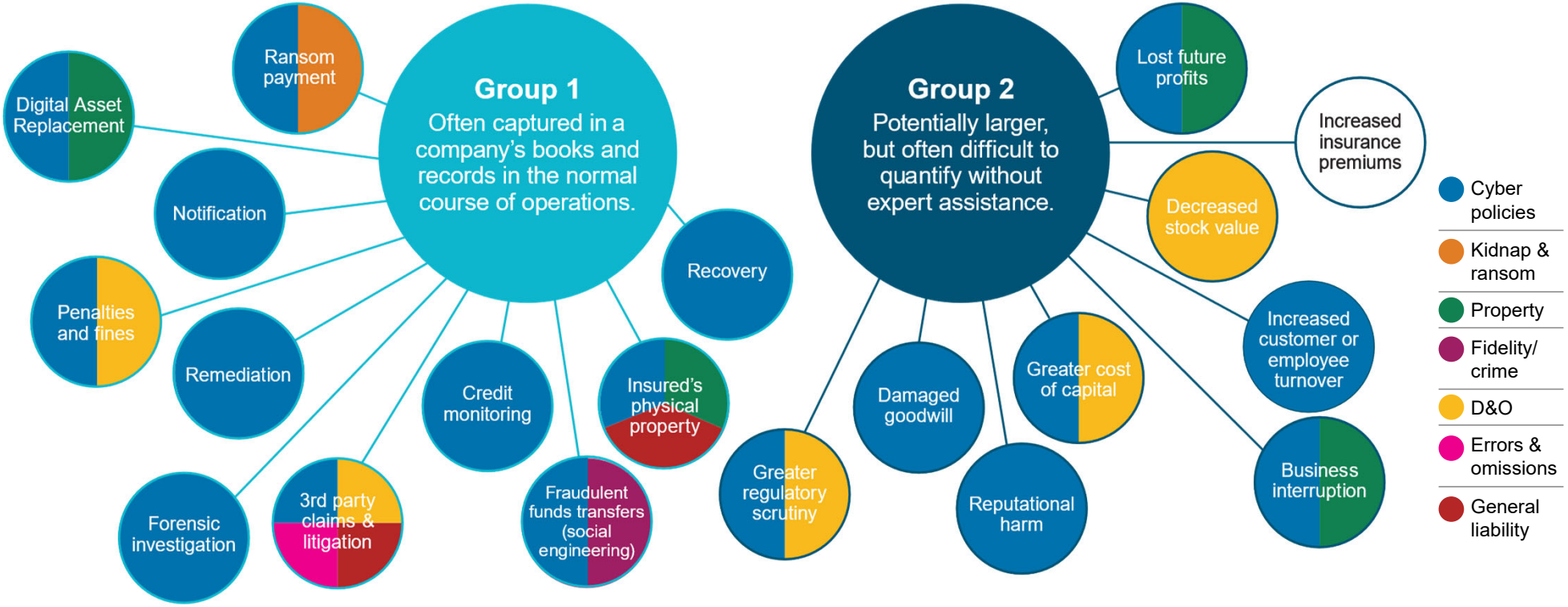
Because cyber damages can be challenging to quantify, companies risk making business, legal, and disclosure decisions based on incomplete estimates of the comprehensive economic impact of a cyber incident.



CRA Charles River Associates

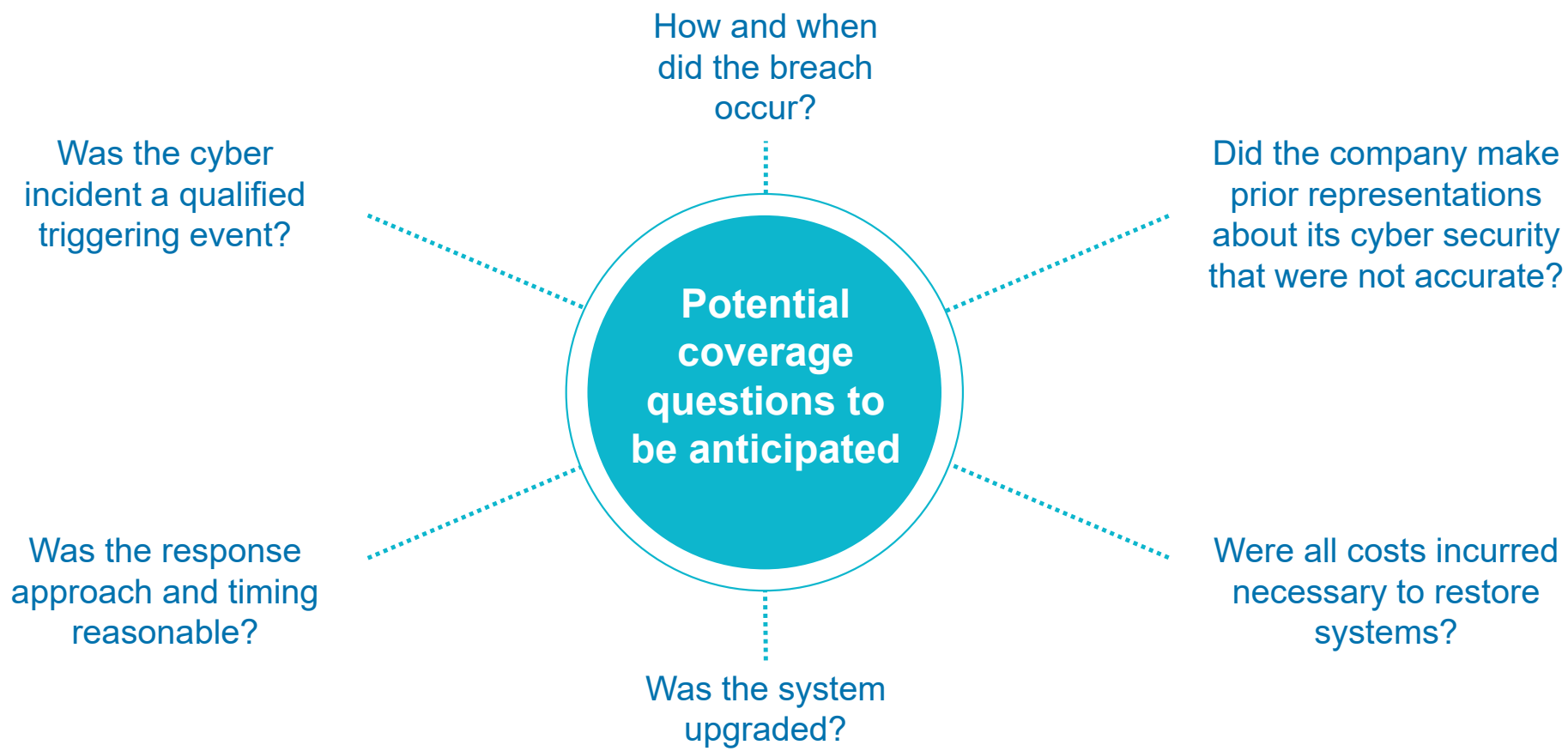
Which insurance policies may cover losses?

Because cyber damages can be challenging to quantify, companies risk making business, legal, and disclosure decisions based on incomplete estimates of the comprehensive economic impact of a cyber incident.



CRA Charles River Associates

Potential coverage questions

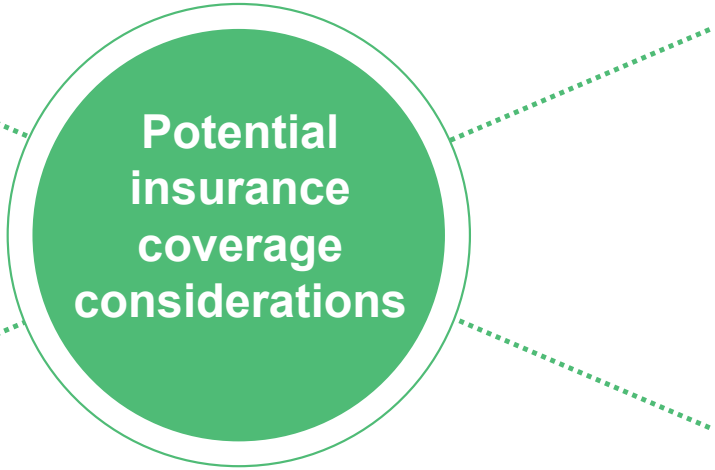


CRA Charles River Associates

Other coverage considerations

Obtaining consent for expenses before incurring them, if required.

Avoiding labels, buzzwords and lingo that inaccurately describe facts and lead to sublimit or other coverage issues.



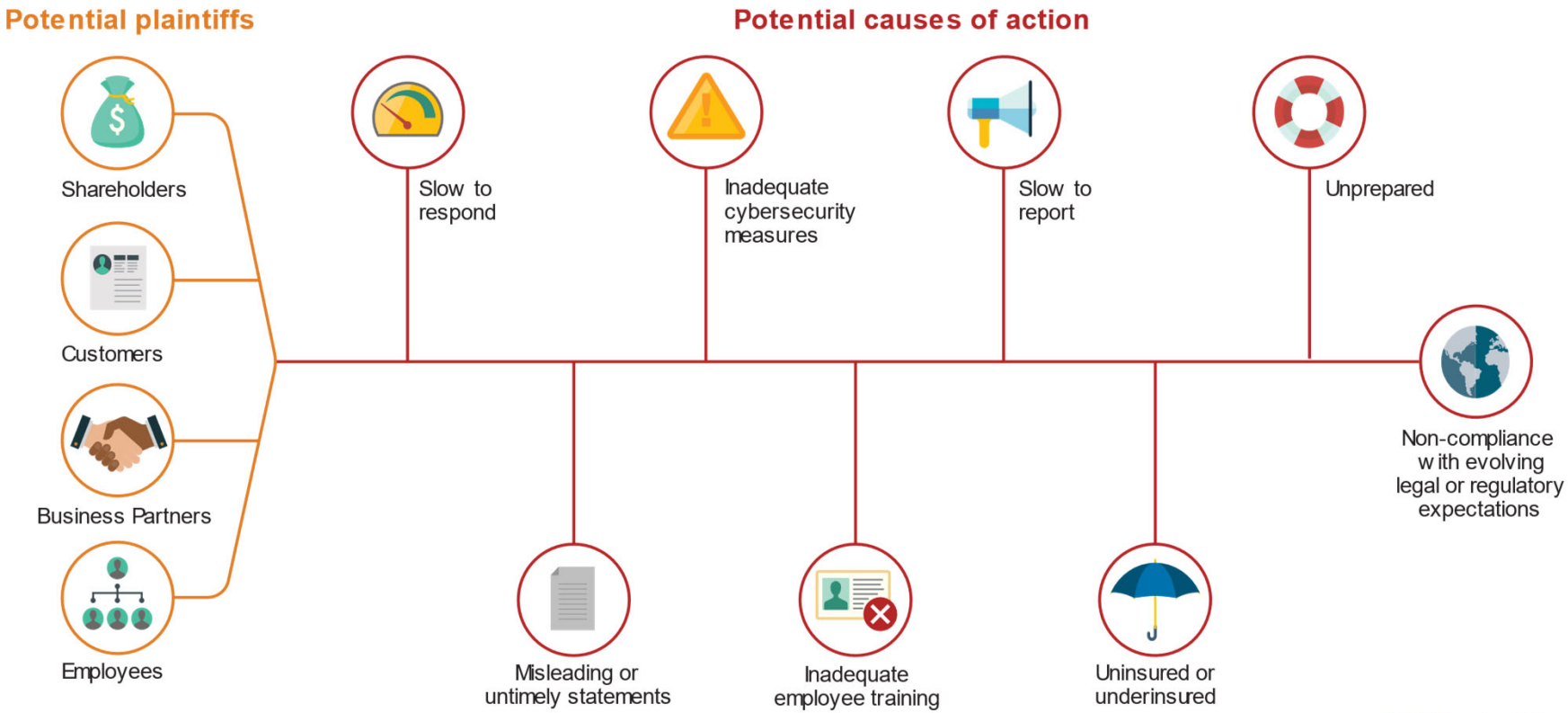
Aligning regulatory filings, insurance coverage arguments/filings, and underlying defense arguments/filings.

Driving the insurance claim process with facts and data.

CRA Charles River Associates

Be prepared for class action litigation

Companies that experience a data breach face class action litigation proceedings, from various parties, and under various causes of action, such as:



CRA Charles River Associates

Regulatory expectations after a data breach

The U.S. Securities and Exchange Commission has outlined the following guidance for registrants who experience a ransomware and/or cybercrime incident in July 2023:

Registrants are required to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.

- Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of such determination, unless delayed by the U.S. Attorney General

Registrants are required to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant.

- Registrants must also describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Appendix

Are big ransom payments a smart response to the global menace of ransomware?

Many companies find it helpful to assess the associated risks through multiple lenses, including:

"Business Risk" lens

Reputation: payments can strengthen the perception among the community of threat actors that the company is an "easy target," potentially increasing the likelihood of being targeted more frequently in the future.

Lack of ROI: payments may not prevent data disclosure or misuse, especially since so much PII is already widely available on the dark web and online. There is also no guarantee that threat actors will return the data or uphold any promises made during negotiations.

Financial impact: payments divert company funds from other shareholder value-creating or risk reducing opportunities, such as the underlying security weaknesses that allowed the attack to occur and may translate into increased cybersecurity insurance premiums.

"Legal and Regulatory Risk" lens

Potential criminal exposure: payments may violate OFAC-enforced regulations, which prohibit transactions with entities on Specially Designated Nationals list or construed as bribes to foreign nationals and thereby a violation of the Foreign Corrupt Practices Act.

Perception of inadequate preparedness: the business decision to make a ransom payment could be second-guessed by regulators and/or the plaintiffs' bar as a failure to adequately foresee, prevent, or prepare for such an attack.

CRA Charles River Associates

Are big ransom payments a smart response to the global menace of ransomware?

"Moral and Ethical Risk" lens

Empowering criminals: payments strengthen threat actors, helping them enhance attack capabilities, and wage more frequent and more serious attacks.Funding criminal activities: proceeds are often used to fund illicit weapons programs and support other actions that undermine democracy and global security.

Brand and trust: payments can damage a company's reputation among those constituents who are opposed to economically supporting criminal activities and increasing the risk of future attacks.

CRA's Forensic Services Practice assists in the prevention, detection, and correction of a broad range of risks and potential misconduct, reaffirming companies' commitment to integrity and exemplary corporate governance. Other recent assignments have included investigating and assessing allegations of financial statement irregularities, fraud, FCPA, and bribery and corruption non-compliance, export controls and sanctions, anti-money laundering, #MeToo issues, theft of trade secrets, ineffectiveness of SOX controls, and cybercrime.

We are grateful for valuable insights from **Lori E. Lightfoot, Esq.**, Senior Consultant to CRA's Forensic Services Practice, in the preparation of this analysis. Lori advises clients in investigating, responding, and navigating through very public crisis situations, drawing upon her collective experiences as the 56th Mayor of the City of Chicago, senior partner at Mayer Brown LLP, Assistant US Attorney in the Northern District of Illinois, and academic assignments at Harvard, the University of Chicago, and the University of Michigan.

Thank you

Kristofer Swanson, CPA/CFF, CAMS, CFE
Vice President and Practice Leader, Forensic Services
Charles River Associates
(312) 619-3313 Direct
kswanson@crai.com

Jordan Kraner, CPA/CFF, CFE
Principal, Forensic Services
Charles River Associates
(312) 619-3319 Direct (Chicago)
(317) 983-1999 Direct (Indianapolis)
jkraner@crai.com

Daniel J. Healy
Co-Chair, Insurance Recovery Group
Brown Rudnick, LLP
(202) 536-1780 Direct
dhealy@brownrudnick.com

Anne Reader
TransUnion
anne.reader@transunion.com

Kevin Small
Counsel
Hunton Andrews Kurth
(212) 309-1226 Direct
ksmall@HuntonAK.com

Jim Tu
McDonalds
james.tu@us.mcd.com

NY RIMS Chapter Meeting

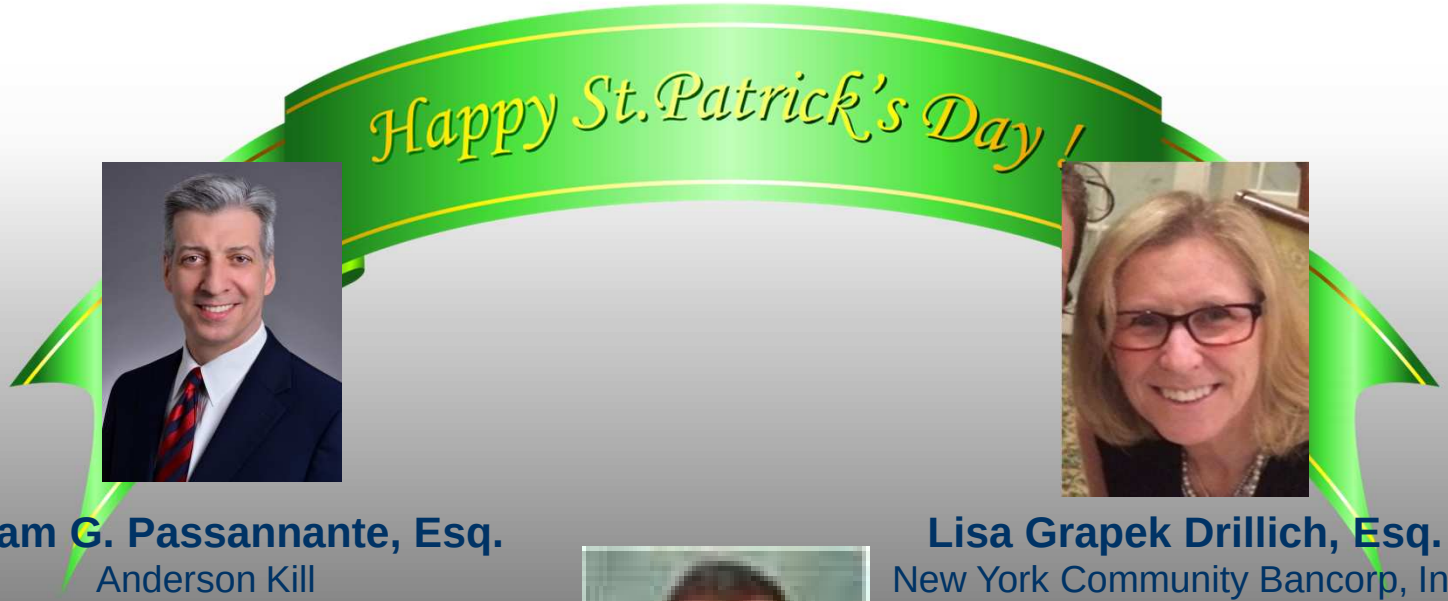
Yale Club
March 17, 2016
8:30 am – 10:30 am

Ten Tips for Getting Claims Paid

Disclaimer

The views expressed by the participants in this program are not those of the participants' employers, their clients, or any other organization. The opinions expressed do not constitute legal advice, or risk management advice. The views discussed are for educational purposes only, and provided only for use during this session.

Your Panel



William G. Passannante, Esq.
Anderson Kill
(212) 278-1328
wpassannante@andersonkill.com

Lisa Grapek Drillich, Esq.
New York Community Bancorp, Inc.
(516) 683-4599
Lisa.Drillich@mynycb.com

R. Damian Brew
Marsh USA, Inc.
(212) 345-2584
Richard.D.Brew@marsh.com

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

Overview

A. Procedural and Process Tips(1-4)

B. Substantive Tips (5-6)

C. People Tips (7)

D. Financial Reality (8-10)

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

1. Underwriting & Application

- What to Do
- Whom to Involve
- When to Do It
- Impact on Subsequent Claims
- Who Should Be Involved
- Selection of Insurer/Policy Form

2. Notice of Event

- Claim, Occurrence or Accident - Circumstance
- Proof of Loss
- Statute of Limitations & Standstill
- Document Everything

3. Defense of Liability Claims

- Who Defends & Why
- Who Pays
- Privilege Issues
- Right to Independent Counsel
- Control of Defense
- Right to Associate
- "Reservation of Rights"

4. Procedural Hurdles

- Cooperation & Information Requests
- Consent to Settle
- Reasonable Defense
- Reasonable Settlement
- Allocation Arguments
- “Suit Limitation”

5. Legal Backdrop

- Forum
- ADR?
- Law on Coverage
- Law Related to Exclusions
- Burden of Proof
- Claims Department Baseline

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

6. Specific Issues

- Dishonesty & Fraud Exclusions
- So-Called "Disgorgement" Defense
- "Follow-Form" Which Doesn't
- Non-Seamless Tower- e.g. ADR

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

7. People Issues in Claims

- Keep Lawyers Out
- Broker Claims Advocates
- Real Decision Makers
- Set the Table for Discussions
- Widen the Number of Issues
- Try to Be Civil
- Group vs. Single Meetings
- Risk Management Involvement

8. Valuing The Claim

- Covered vs. Non-Covered
- Amount of Verdict or Settlement
- Allocation of Loss Among Multiple Policies – Horizontal & Vertical
- Impact of Legal Backdrop
- Value of Court Ruling & Jury Verdict
- Percentages
- Good Faith & Fair Dealing

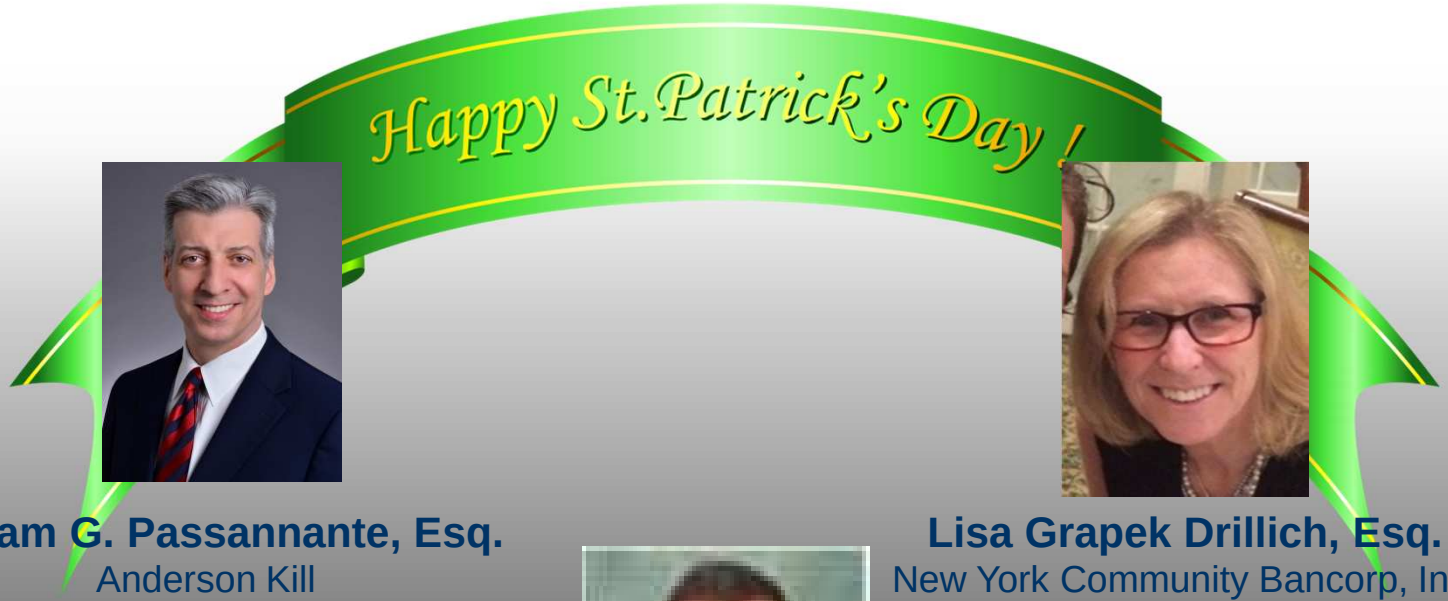
9. Financial Reality

- Premium
- “Float”
- Industry Profit
- Broker’s Value and Leverage
- Scope of Released Claims

10. Policyholder's Reality

- Want Real, Honest Risk-Transfer
- Seek Reasonable Premium
- Want Good Service
- Dislike Surprises
- Timing

Your Panel



William G. Passannante, Esq.
Anderson Kill
(212) 278-1328
wpassannante@andersonkill.com

Lisa Grapek Drillich, Esq.
New York Community Bancorp, Inc.
(516) 683-4599
Lisa.Drillich@mynycb.com

R. Damian Brew
Marsh USA, Inc.
(212) 345-2584
Richard.D.Brew@marsh.com

ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

What Steps Businesses Can Take After CrowdStrike Failure

By **Daniel Healy** (August 13, 2024)

Daniel Healy

On July 19, businesses around the globe suffered what has been described as a meltdown.

The businesses were all users of Microsoft Corp. operating systems that were supported by CrowdStrike. Ironically, CrowdStrike Holdings, Inc. is a provider of security software intended to protect computer systems from malware, hackers and other threats.

However, on July 19, CrowdStrike pushed out a security update containing software code that caused the Microsoft platforms it is intended to protect, to crash repeatedly in a loop and lose all functionality.

Businesses Affected

In the U.K., the FTSE 100 slumped due to the outage of so many large companies.[1] Airlines received the most attention because the complete failure of computer systems for so many airlines resulted in flight cancelations, leaving passengers stranded in airports around the world.

British Airways PLC reported canceling approximately 131 flights from July 19-21.[2] Across major airlines, over 4,000 flights were canceled on July 19 alone, and over 11,000 from July 19-21. For many airlines the problems lasted through the following week.

NHS hospitals and other medical providers were prevented from carrying out vital business activity and from accessing information in order to offer medical care.[3] Likewise, some emergency response operators' call centers lost operation.

Financial systems suffered inoperability, including trading platforms, banks, retail payment systems and other Microsoft-based transactional systems and platforms. The financial cost of the outage remains to be calculated.

There are reports that more 311,000 instances of global outages were reported before the software was repaired.[4] The impact of such business interruptions can create far-reaching ripple effects. Not all of them will be resolved quickly.

In contrast to the widespread, global effect of the software failure, the number of affected devices was apparently relatively small. Microsoft estimated that 8.5 million Windows devices worldwide were affected.[5] Compared to the number of devices in the world, that is a low figure.

Similarly, CrowdStrike claims that it serves approximately 29,000 customers. On a global basis, that is not a staggeringly large number of affected businesses, even assuming all of them were completely shut down. One of the issues may be the size and importance of the businesses that owned or relied upon those devices.

Additionally, the extent to which computer systems overlap and the multiple layers of reliance that stem from a single platform may be key to how the meltdown immediately

affected so many services, people and transactions around the globe — and did so for a prolonged period of time.

For example, in the U.K., hospitals were directly affected, losing the ability to process patients' records. One result was that prescriptions were not processed and sent to pharmacies, some of which were also hampered by the meltdown.

Even when computer systems were back online, pharmacies were overrun with backed-up prescription orders that could not be filled in a timely manner. Some pharmacies reported that the problem lasted days.

While many affected businesses have now returned to full operation, recovery is more complicated than simply returning to full functionality. Businesses may need to investigate which processes were nonfunctional or impaired and what services, transactions or other deliverables failed.

Similarly, determining what services were provided only after extensive delay, some of which may have defeated the purpose of the service, will be important.

Understanding What Happened

An initial step is understanding what happened and how it caused the outage. CrowdStrike reported in an online blog that a security software update contained a logic error. It posted that it had released "a sensor configuration update to Windows systems. Sensor configuration updates are an ongoing part of the protection mechanisms of the Falcon platform."[6]

The platform provides real-time information about evolving threats to computer systems. The one released on July 19 was a rapid response content update pushed to customers early in the morning, but it contained an error that instructed the update to attempt to read material either before or after the intended buffer of memory in the operating system.

CrowdStrike identified the specific file as a so-called channel file, and stated that "the impacted channel file in this event is 291, and will have a filename that starts with 'C-00000291-' and ends with a .sys extension." Channel files were used here to distribute dynamic files that work in a cloud environment and can detect the most current threat. The purpose is to provide updates to security software as threats evolve so that the software can detect the latest threats.

Here, the channel file contained a logic error that crashed the operating system into which it was deployed. The result was a system crash, and rebooting the Microsoft system triggered another crash, leading to a complete system failure.

Unlike other major cyber incidents, there was no third-party threat actor intending to release malware that crippled computer systems worldwide, or who hacked into a computer system and exfiltrated data. Instead, a security software vendor released what it states it expected to be a security enhancement, which resulted in worldwide system failure.

Although not a typical malware or data breach, the losses suffered by businesses are similar in many ways to a ransomware attack, including disrupted operations, recovery costs and legal fees, plus loss of revenue, opportunities, and consumer and investor confidence. All of these can lead to contractual and indemnity issues.

The interconnectivity demonstrated by the technological failure has a legal backdrop that consists of legal agreements that set forth obligations, responsibilities and waivers of rights. Agreements typically follow the software and the services being provided with the software.

Since the software owner or provider is in many instances not the provider of services using the software — for example, Microsoft provided the operating system that hotels use to provide hospitality services — there is a multilayered set of agreements and legal obligations. These layers of legal obligations may make for complex issues when working through the financial recovery for many businesses.

Software is typically licensed and involves an agreement. The agreements usually include indemnity provisions, limitations on liability and insurance requirements. Such provisions are intended to provide clarity and assign liability in the event of an incident and loss involving the software.

Software, in turn, is used by businesses to provide services as well as goods. Major providers of travel, healthcare and financial services were heavily affected by the outage and were unable to provide services.

These services often have agreements dictating the assignment of liability. For business-to-business relationships, such services most likely have indemnity and insurance provision. For consumer relationships, such as hotel guests, airline passengers and banking clients, the number of written agreements will vary. Common law will also provide for the assignment of liability where agreements do not.

Quantifying Losses

In the coming weeks, many businesses will be working to quantify the loss the suffered and expenses incurred due to the outage. It may transpire that actions beyond the software outage itself exacerbated the loss, which may lead to claims that other parties are liable.

In addition, the end users, whether consumers or other businesses, of the services that were not provided will have claims against the business expected to provide the services. With British Airways, for example, passengers do not have a relationship with CrowdStrike, but with the airline. The tiers of relationships and the ripple effect of the loss will lead to multilayered disputes over liability.

Affected businesses should locate relevant contracts and agreements, as well as their insurance policies, as the starting point for legal recovery. The monetary component of recovery may come from more than one source.

For example, many businesses may have indemnity that covers part of their loss and insurance coverage, possibly under policies procured by another business, which covers another portion of the loss. Those business also should look at their own insurance policies.

Insurance Considerations

Cyber insurance policies may be the first place that businesses look for a recovery. Many businesses already are asking about business interruption coverage, which often applies when unexpected circumstances leave a business unable to perform at normal levels.

Business interruption coverage is found in cyber policies and property policies, most commonly, and businesses should review their property and cyber cover to determine

whether those policies apply. If so, they should check whether such cover applies in order to reimburse for losses stemming from a business's inability to generate revenue and profits.

There are a number of considerations, including whether the policy applies to the loss. Both cyber and property policies can apply where computer systems are affected by a loss, but it will depend on the policy wording as to whether a breach, physical damage or cyber incident contemplated by the policy took place. It is worth considering that a third party sent unrequested software to the businesses whose computer systems crashed.

Additionally, many business interruption coverage provisions have waiting periods. Such provisions can state that cover does not kick in until the interruption lasts longer than a certain time period, such as 72 hours. However, in many policies that provide cover relating to computer systems, there are alternative provisions. Those provisions can focus on the amount of revenue or profit lost, rather than the length of the interruption after the waiting period.

On the other hand, if the cover applies, many such policies also have contingencies. It is similar to business interruption cover and can include cover for when a supplier is unable to supply a product or service vital to the policyholder's ability to provide its services.

Also, similar provisions might provide that when a key venue or nearby property, known as an attraction property, that drives the policyholder's business is shut down, then the policyholder has cover. Here, if a key supplier or covered attraction property is affected, businesses should check their policies for coverage.

Any loss scenario involving the failure to provide, or to properly provide, services can implicate an errors and omissions liability, or E&O, policy. Those policies can be like malpractice policies, providing cover when services are not provided to customers as agreed.

They also may provide cover when the services were not provided in accordance with a contract. For example, if certain professional services were not performed as required or were performed improperly due to the outage, E&O coverage for wrongful acts involving professional services could apply.

Many E&O policies specifically provide cover for computer incidents and can be referred to as E&O tech policies. Businesses should find out the facts of their loss and pursue coverage under any applicable policies.

Practical Takeaways

Affected businesses should not ignore policies they may have in place. They should give notice under any potentially applicable policies. They should also read the wording of their policies and not rely on generalized assumptions about what is covered.

For example, there is no form policy for cyber insurance, and it can differ from one policy to another. This means that the same insurance company can use different wording in each of its policies.

Not all policies require a hack or the typical event to be triggered. Such policies often contain an array of coverage provisions, some first-party coverage and some third-party coverage — that is, liability coverage. The provisions are not all based on the assumption that a system was hacked.

When employees are tricked by third parties, there is no system breach, but data or money is taken and there are provisions providing coverage for such incidents. Businesses should not assume there is no cover just because they were not hacked. [original text read: Businesses should not assume there is no coverage just because they do not believe they were not hacked]

Other policies may apply. They could include event cancelation policies, travel insurance and potentially directors and officers liability, depending on the claims at issue.

After gathering and reviewing their contract and insurance policies, businesses should communicate in writing, document their losses and push back on early refusals to cover losses. It may be an uphill battle because this incident was not an expected issue, but that is exactly why indemnity provisions and insurance policies are so important.

Daniel Healy is a partner at Brown Rudnick LLP.

[1] "Wall Street and European stocks lower as Microsoft outage wreaks havoc," Harding, LaToya, Yahoo Finance.

[2] "CrowdStrike travel chaos: Airlines struggling back to normal operations," Grant, John, OAG: https://www.oag.com/blog/crowdstrike-travel-chaos-airlines-struggling-back-to-normal-operations.

[3] "Second NHS IT system confirmed to be affected by CrowdStrike issues," Jones, Conor, The Register: https://www.theregister.com/2024/07/19/crowdstrike_update_nhs_it_outages.

[4] "What we know about the computer update glitch disrupting systems around the world," Bobby Allyn, Brian Mann, Bill Chappell and Fatima Al-Kassab, NPR: https://www.npr.org/2024/07/19/g-s1-12222/microsoft-outage-banks-airlines-broadcasters.

[5] "Microsoft says 8.5 million devices were affected by the CrowdStrike bug or 'less than one percent of all Windows devices' as new details emerge on Friday's tech meltdown": Edser, Anne, PS Gamer.

[6] See CrowdStrike Blog at https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details.

Insurance Policy Takeaways From UK Lockdown Loss Ruling

By **Daniel Healy** (March 22, 2024)

Daniel Healy

On Feb. 9, the High Court of Justice of England and Wales handed down a decision in Unipolsai Assicurazioni SpA v. Covéa Insurance PLC, which addressed an unusual reinsurance dispute concerning coverage for the initial COVID-19 lockdown.[1]

The decision is uncommon, in part because reinsurance disputes in England are most often decided in confidential arbitration, not in public courtrooms.

The case also presented a dispute about what many British insurance companies refer to as "non-damage" COVID-related claims, suggesting that the claims involved losses wherein the property did not suffer structural harm, yet there is reinsurance coverage. The coverage at issue was business interruption coverage for the period of the lockdown due to government orders, regardless of whether the business property was structurally damaged.

This article covers the key arguments and rulings from the case. The reinsurance companies appealed from arbitration rulings that required them to provide coverage to their insureds, namely the insurance companies.

The key issues included whether the rise in COVID-19 cases leading up to the issuance of a lockdown order were a covered catastrophe, and, if yes, whether the so-called hours clause limited the recovery after the order to a set number of hours' worth of loss. It is important for policyholders to keep in mind how the insurance companies argued for coverage and, even if some of the words differ, the concepts they relied upon in obtaining reinsurance coverage.

What's at stake?

For policyholders, reinsurance disputes present a further opportunity to see insurance companies argue against their reinsurance companies to obtain reinsurance coverage.

Insurance companies seeking reinsurance coverage largely have to argue insurance coverage positions that are more akin to the coverage positions that policyholders typically argue in seeking insurance recoveries compared to typical insurance company positions. Insurance companies argue for coverage under their reinsurance policies, refuting coverage denials by their reinsurers.

High Court decisions present interesting insurance disputes because the policy wording often drives the decisions.

The wording in English and London-based policies often differs slightly from the typical wording in U.S. equivalents, even though they may have been intended to have the same meaning. However, this decision involves reinsurance policy provisions and wording from London policies that are not exactly the same as domestic, U.S. insurance coverage disputes.

The arguments of the reinsured, i.e., insurance companies in the shoes of policyholders,

against the reinsurers, i.e., the insurer of the insurance companies, rely on policy wording that is not entirely the same as, but, in many ways, serves the same or similar purposes as, the terms of U.S. policy provisions.

What was the case about?

The recent case is captioned but involved two disputes. One was between Unipolsai Assicurazioni, or UnipolRe, and its reinsured Covéa Insurance, and the other was between General Reinsurance AG, or GenRe, and its reinsured Markel International Insurance Co. Ltd.

Both Covéa and Markel pursued coverage claims against their reinsurance companies. The claims were for coverage that was paid when nurseries and child care centers in the U.K. were forced to shut down at the onset of the COVID-19 pandemic.

As described in the decision, the U.K. government shut down a range of businesses though an order issued on March 18, 2020. The order required the closure of nurseries and child care centers. That order was renewed on April 16, 2020, and again on June 23, 2020, and remained in place until the Prime Minister Boris Johnson lifted it on July 4, 2020. While in place, it required full closure.

Prior to the time it was lifted, a phased reopening had begun that started on June 1, 2020. The somewhat complex timeline did not make loss calculation typical. Thus, the closed businesses sought coverage based on the time each was closed by government order, despite the fact that the locations had not demonstrated the presence of COVID-19 on the property.

The insurance issues before the High Court on appeal were novel. For the first time, the High Court determined the meaning of "catastrophe," rejecting the reinsurance companies' contentions that there had been no catastrophe for which reinsurance coverage could be paid.

The arguments by the insurance companies seeking coverage were that the order on March 18, 2020, constituted a catastrophe, and that the pandemic itself involved an outbreak of disease that constituted a catastrophe.

Additionally, the reinsurance companies argued that, even if there had been a catastrophe, the so-called hours clause limited the recovery to the 168 hours immediately following the government order. The clause sets time limits on the period for which coverage will be provided, and the issue involved whether the clause limited the time that loss occurrences took place, such as increasing COVID-19 cases, or the period of indemnity.

COVID-19 was considered a catastrophe under the policies.

The appeal was based on Markel's and Covéa's successful arbitrations against GenRe and UnipolRe, in January 2023 and June 2023 respectively. In both arbitrations, the insurance companies successfully established that a catastrophe had taken place. However, the separate arbitrations ruled on different arguments.

The Covéa policies provided coverage for property loss, including business interruption for the time a business is unable to operate due to property damage. The High Court decisions stated that coverage was for "the wide miscellany of risks that are commonly found in commercial cover written by a property department … [including] … business interruption

caused by a peril other than physical damage to insured property."[2]

The arbitration panel labeled the coverage as being for "non-property damage business interruption."

The Covéa arbitration panel had found that the "exponential increase" in COVID-19 cases over three weeks in March 2020 was a disaster "of sudden onset" that constituted a catastrophe under the policy wording.[3]

The Markel policies had different wording and provided two types of coverage grants. One provided coverage for "closure or restriction in the use of the premises due to the order or advice of the competent local authority as a result of … an occurrence of an infectious disease."

The other provided for when access to property is:

> prevented or hindered by (a) physical loss or damage to property in the Vicinity of the Premises …. [and] any action of Government or Police or Local Authority due to an emergency which could endanger life or neighbouring property … [and] any occurrence of a Notifiable Disease … at Your Premises … which causes restrictions on the use of Your Premises on the order or advice of the competent local authority.[4]

The High Court also noted that the Markel arbitration panel had held that the order on March 18, 2020, and the COVID-19 outbreak leading to it constituted a catastrophe for purposes of the treaty reinsurance and in general.[5]

On appeal, the reinsurance companies argued that the cases of COVID-19 leading to the orders and the order on March 18, 2020, and subsequent orders, did not constitute a catastrophe under the reinsurance policies. The reinsurers argued that a "catastrophe" is something that causes physical damage to property, requires a sudden and violent happening, and must be an event or occurrence that has a unity of "time place and way."[6] They also suggested that the lockdown order mitigated and did not cause damage.

The High Court applied a reasonableness standard in interpreting the policy language. That standard is the meaning the language would convey to a reasonable person having all the background the parties had at the time of contracting.

For policyholders, this type of standard can present a difference in how it is applied to each party. Arguably, that difference may not apply where there are two insurance companies entering into the contract.

The High Court further relied on dictionary definitions[7] and the wording of the reinsurance policies to find that a "catastrophe" did not need to meet the requirements set forth by the reinsurers.[8]

The decision is important because it demonstrates that the coverage in aggregation clauses — intended to gather a number of events into a single loss — does not add requirements to the type of covered loss. The provisions should fulfill their purpose of stating how events can form a single loss. Applying the provision here meant that Markel and Covea had suffered losses that combined reach coverage under the reinsurance treaties.

The hours clause did not eviscerate coverage.

The Covéa and GenRe also argued that the hours clause limited coverage to the 168 hours following the order on March 18, 2020. The High Court again disagreed. It focused on the wording and the purpose of the provision.

Many insurance coverage cases involve the meaning of the term "occurrence." Here, the key wording at issue grew out of a London market form called the LPO 98. It defined "loss occurrence" to include individual losses "arising out of and directly occasioned by one catastrophe."

But the provision continued on to limit the duration of a loss occurrence to a number of hours for certain, specified perils, and to 168 hours for any other peril, such as COVID-19. Last, the provision stated that "no individual loss from whatever insured peril" outside those periods is part of the loss occurrence.

The key issue centered on the policy provision that the duration of loss occurrence of any nature is limited to 168 consecutive hours, as there was no dispute regarding other named perils. The wording sets time limits by hours on the scope of coverage to be paid by a reinsurance company for a loss. The concept is that the loss is treated as a single event, even if the event had multiple parts.

The High Court noted that the author of the form had described it as "one of the most difficult and contentious clauses in any catastrophe wording," and predicted that courts might have difficulty interpreting it as actually intended.

Apparently, after confusion about the scope of coverage for a snowstorm in the U.K. that ended with multiple thaws that created losses from water damage, the industry developed wording to address whether such circumstances were single or multiple events. The High Court explained that the clause is used to aggregate loss occurrences from one catastrophe. Highlighting this approach, the court quoted a treatise that noted the origins of the wording:

> It will be noted that the word 'event' was abandoned in favour of the word "catastrophe" to make it clear that the intention was to cover happenings that were short, sharp and devastating; this indeed was historically the correct analysis of catastrophe covers, which are commonly believed to have originated after the San Francisco earthquake of 1906.

The High Court found that the hours clause meant that the clause limited the amount of coverage based on the duration of the loss occurrence and not the duration of the individual loss. No other loss from any peril that occurs outside the specified hours will be included in the event or catastrophe for coverage.

Thus, the 168 hours related to the timing of the increase in COVID-19 cases and the issuance of the order on March 18, 2020, and not the length of time the nurseries and child care centers were shut down.

Again, looking at other policy provisions, the High Court noted that other provisions address the length of the loss, such as limitations on the indemnity period. The period of indemnity was not limited to 168 hours, and the recovery was for the resulting loss, not an arbitrary number of hours.

The High Court's decision is a pro-coverage ruling. While it is in the reinsurance context and based on U.K.-based policy forms, it provides a number of analyses helpful to U.S.

policyholders.

The decision analyzes the reinsurance policies and highlights how the different policy provisions — together with the ordinary meaning of the words and combined with the context in which provisions were originally drafted — demonstrates that they have clear meaning intended to provide coverage. Policyholders should take note and keep these principles in mind.

Daniel J. Healy is a partner at Brown Rudnick LLP.

[1] Unipolsai Assicurazioni SpA v. Covéa Insurance PLC, [February 9, 2024] EWHC 253 (Comm).

[2] High Court Decision ¶7.

[3] High Court Decision ¶22.

[4] High Court Decision ¶26.

[5] High Court Decision ¶32.

[6] High Court Decision ¶64.

[7] High Court Decision ¶68.

[8] High Court Decision ¶74, et seq.

2024 IL App (1st) 231712

Appellate Court of Illinois, First District,
Second Division.

TONY'S FINER FOODS ENTERPRISES, INC., Plaintiff-Appellee,
v.
CERTAIN UNDERWRITERS AT LLOYD'S, LONDON, Subscribing to Policy Nos. MPL2183838.18 and MPL2183838.19, Defendants-Appellants.

No. 1-23-1712
|
Opinion Filed September 10, 2024

Synopsis

Background: Employer brought action against liability insurer for declaratory judgment that insurer owed duty to defend employer under Cyber, Data Risk, and Media Insurance policies in employee's class action alleging violations of Biometric Information Privacy Act in connection with requirement that employees scan fingerprints into third-party's database and use fingerprints to clock in and out of work. The Circuit Court, Cook County, Joel Chupack, J., entered summary judgment in favor of insured. Insurer appealed.

Holdings: The Appellate Court, Rena M. Van Tine, J., held that:

alleged violations of Act were not "data breach" or "security failure" covered by policies, and

exclusion related to loss based upon or arising out of any actual or alleged collection of information by employer barred coverage.

Reversed and remanded with directions.

Reyes, J., dissented and filed opinion.

Procedural Posture(s): On Appeal; Motion for Summary Judgment.

Appeal from the Circuit Court of Cook County. No. 22 CH 9420, Honorable Joel Chupack, Judge, presiding.

Attorneys and Law Firms

Geoffrey J. Repo, of Gordon Rees Scully Mansukhani LLP, of Chicago, for appellants.

Eamon P. Kelly and Clayton Faits, of Sperling & Slater LLC, of Chicago, for appellee.

OPINION

PRESIDING JUSTICE VAN TINE delivered the judgment of the court, with opinion.

***1** ¶ 1 Defendants Certain Underwriters at Lloyd's, London, subscribing to policy Nos. MPL2183838.18 and MPL2183838.19 (Lloyd's), appeal from the circuit court's grant of summary judgment in favor of plaintiff Tony's Finer Foods Enterprises, Inc. (Tony's). The circuit court ruled that Lloyd's has a duty to defend Tony's in an underlying class action filed against Tony's by its employees, which alleges violations of the Biometric Information Privacy Act (Act) (740 ILCS 14/1 *et seq.* (West 2018)). On appeal, Lloyd's argues that it has no duty to defend Tony's because (1) the allegations of the underlying Act lawsuit do not even potentially fall within the coverage of the insurance policy at issue and (2) Tony's did not timely report the underlying Act lawsuit to Lloyd's. For the following reasons, we reverse and remand with directions that the circuit court enter summary judgment in Lloyd's favor on the issue of duty to defend.

¶ 2 I. BACKGROUND

¶ 3 A. The Underlying Act Lawsuit

¶ 4 On December 19, 2018, Charlene Figueroa filed a class action lawsuit against Tony's and on April 19, 2019, she filed the amended complaint that is relevant to this appeal. [1] Figueroa alleged that she worked for Tony's from March 8, 2017, to September 17, 2018. During that time, Tony's required employees to scan their fingerprints to clock in and out of work. Employees used fingerprint recognition software provided by a timekeeping company called Kronos,

which also maintained a database of employees' fingerprints. Figueroa alleged that Tony's violated the Act by failing to (1) publish a schedule for the permanent deletion of employees' biometric data (*id.* § 15(a)), (2) obtain employees' consent to the collection of their biometric data and provide a written disclosure explaining why and for how long Tony's retained their biometric data (*id.* § 15(b)), and (3) obtain employees' consent to disclose their biometric data to Kronos and other unknown third parties (*id.* § 15(d)(1)).[2] Figueroa served Tony's in the underlying Act lawsuit on January 8, 2019. Tony's tendered the Act complaint to Lloyd's on March 22, 2019, seeking defense and indemnification in the underlying lawsuit pursuant to two insurance policies that Tony's purchased from Lloyd's.

[1] Figueroa's original and amended complaints are largely the same, but the amended complaint controls because it does not refer to or adopt the original complaint. See *Eberhardt v. Village of Tinley Park*, 2024 IL App (1st) 230139, ¶ 86, —— Ill.Dec. ——, —— N.E.3d —— (citing *Bowman v. County of Lake*, 29 Ill. 2d 268, 272, 193 N.E.2d 833 (1963)). The primary difference between the two pleadings is that the original complaint alleged one count for violation of the Act and one count for negligence whereas the amended complaint alleges three counts for violation of the Act and no negligence count.

[2] Figueroa has never named Kronos as a defendant.

¶ 5 B. The Insurance Policies

¶ 6 Lloyd's issued two insurance policies to Tony's, both titled "Cyber, Data Risk, and Media Insurance." The first policy ran from March 15, 2018, to March 15, 2019 (2018 policy), and the second policy ran from March 15, 2019, to March 15, 2020 (2019 policy). The two policies are essentially identical except for the periods of time they covered, so we will discuss them as a single policy unless a distinction between the two is necessary.

***2** ¶ 7 Relevant here, the policy provides coverage for "loss incurred by [Tony's] *** resulting from a data breach, security failure, or extortion threat that first occurs on or after the retroactive date and is discovered by [Tony's] during the policy period." Loss includes "claim expenses, damages, and PCI fines and assessments because of a claim made against [Tony's]." The policy sets out the following definitions:

> "Data breach means the acquisition, access, or disclosure of personally identifiable information or confidential corporate information by a person or entity, or in a manner, that is unauthorized by [Tony's].
>
> ***
>
> Extortion threat means a threat from a third-party to commit an intentional attack against [Tony's] website or computer systems or publicly disclose confidential corporate information or personally identifiable information misappropriated from [Tony's] if money, securities, or other property of value is not paid.
>
> ***
>
> Security failure means any failure by [Tony's] or by others on [Tony's] behalf (including [Tony's] subcontractors, outsourcers, or independent contractors) in securing [Tony's] computer system."

¶ 8 The policy excludes certain claims from coverage. Relevant here, an exclusion provision states that:

> "This policy does not apply to and [Lloyd's] will have no obligation to pay any loss, damages, claim expenses, or other amounts:
>
> 1. based upon or arising out of any actual or alleged:
>
> a. collection of information by [Tony's] (or others on [Tony's] behalf) without the knowledge or permission of the persons to whom such information relates; however, this exclusion will not apply if no board member, trustee, director, or officers (or equivalent position) of [Tony's] knew or had reason to know of such conduct; or
>
> b. use of personally identifiable information by [Tony's] (or others on [Tony's] behalf) in violation of law."

¶ 9 C. This Declaratory Action

¶ 10 Lloyd's denied coverage on June 6, 2019, based on Tony's failure to notify Lloyd's of the underlying Act lawsuit during the 2018 policy period. According to Lloyd's, the policy required such notice to trigger coverage. On September 22, 2022, Tony's filed this declaratory judgment action against Lloyd's, alleging that Lloyd's had a duty to defend Tony's in

the underlying Act lawsuit.[3] The parties filed cross-motions for summary judgment. Tony's motion argued that Lloyd's was not permitted to flatly deny coverage; rather, Lloyd's had to either (1) defend the underlying Act lawsuit pursuant to a reservation of rights or (2) seek its own declaratory judgment that it had no duty to defend. Lloyd's motion contended that Tony's failed to provide notice of the underlying Act lawsuit to Lloyd's during the 2018 policy period. Lloyd's also argued that the allegations of the underlying Act lawsuit did not even potentially fall within the coverage provisions of the insurance policy.

[3] Tony's initially named "Hiscox Inc." as the insurance provider defendant in this declaratory judgment action. Lloyd's brought this error to the circuit court's attention and the court amended the caption to replace "Hiscox Inc." with Lloyd's.

¶ 11 The circuit court granted summary judgment in Tony's favor. The court found that Lloyd's had a duty to defend Tony's because the allegations of the underlying Act lawsuit potentially fell within the policy's coverage. The record is void of any reason for this conclusion. The court also found that Lloyd's was estopped from asserting policy defenses because Lloyd's failed to defend Tony's in the underlying Act lawsuit pursuant to a reservation of rights and failed to file its own declaratory action. Lloyd's filed a motion to reconsider, which the circuit court denied.

***3** ¶ 12 Lloyd's timely appealed.

¶ 13 II. ANALYSIS

¶ 14 Lloyd's argues that the circuit court erred in granting summary judgment for Tony's because (1) the allegations of the underlying Act lawsuit do not even potentially fall within the insurance policies' coverage and (2) Tony's did not report the underlying Act lawsuit to Lloyd's during the 2018 policy period.

¶ 15 Summary judgment should be granted when the pleadings, admissions, depositions, and affidavits on file, viewed in the light most favorable to the nonmovant, establish that there is no genuine issue of material fact, and that the movant is entitled to judgment as a matter of law. 735 ILCS 5/2-1005(c) (West 2018); *Thounsavath v. State Farm Mutual Automobile Insurance Co.*, 2018 IL 122558, ¶ 15, 423 Ill.Dec. 150, 104 N.E.3d 1239. We review the circuit court's grant of summary judgment *de novo* (*Thounsavath*, 2018 IL 122558, ¶ 16, 423 Ill.Dec. 150, 104 N.E.3d 1239), meaning that we perform the same analysis as the circuit court (*Galarza v. Direct Auto Insurance Co.*, 2022 IL App (1st) 211595, ¶ 33, 463 Ill.Dec. 291, 209 N.E.3d 409). We also review this matter *de novo* because it involves the interpretation of insurance policies, a task that concerns questions of law. See *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 30, 451 Ill.Dec. 1, 183 N.E.3d 47.

¶ 16 When interpreting an insurance policy, a court's primary objective is to ascertain and give effect to the intentions of the parties as expressed by the language of the policy. *Valley Forge Insurance Co. v. Swiderski Electronics, Inc.*, 223 Ill. 2d 352, 362, 307 Ill.Dec. 653, 860 N.E.2d 307 (2006). If the policy language is unambiguous, we enforce it as written unless doing so would violate public policy. *Schultz v. Illinois Farmers Insurance Co.*, 237 Ill. 2d 391, 400, 341 Ill.Dec. 429, 930 N.E.2d 943 (2010). But if the policy language is susceptible to more than one meaning, then it is ambiguous, and we must construe it strictly against the insurer. *Pekin Insurance Co. v. Wilson*, 237 Ill. 2d 446, 456, 341 Ill.Dec. 497, 930 N.E.2d 1011 (2010). Additionally, we construe provisions that limit or exclude coverage liberally in favor of the insured and against the insurer. *Id.* We also construe the policy as a whole and account for the type of insurance purchased, the nature of the risks involved, and the overall purpose of the policy. *Id.*

¶ 17 As an initial matter, Tony's argues that Lloyd's refusal to defend the underlying Act lawsuit was a breach of the duty to defend; therefore, Lloyd's is estopped from raising any coverage defenses. When an insured party tenders defense of a claim to its insurer and the insurer believes that the claim is not covered by the insurance policy, the insurer cannot "simply refuse to defend the insured." *Employers Insurance of Wausau v. Ehlco Liquidating Trust*, 186 Ill. 2d 127, 150, 237 Ill.Dec. 82, 708 N.E.2d 1122 (1999). Rather, the insurer must either (1) defend the underlying lawsuit under a reservation of rights or (2) seek a declaratory judgment that no coverage exists under the terms of the policy. *Id.* If the insurer does not take either of these actions and is later found to have wrongfully denied coverage, it has breached its duty to defend. *Id.* at 150-51, 237 Ill.Dec. 82, 708 N.E.2d 1122. As a result, the insurer is estopped from later asserting any policy defenses to coverage, even if those defenses may have been successful in the absence of the breach. *Id.* at 151-52, 237 Ill.Dec. 82, 708 N.E.2d 1122. However, estoppel applies only when an insurer breached its duty to defend, so a court

must first determine whether the insurer has a duty to defend and whether it breached that duty. *Id.* at 151, 237 Ill.Dec. 82, 708 N.E.2d 1122.

***4** ¶ 18 We evaluate an insurer's duty to defend by comparing the allegations of the underlying complaint to the language of the insurance policy. *Uhlich Children's Advantage Network v. National Union Fire Co. of Pittsburgh*, 398 Ill. App. 3d 710, 716, 340 Ill.Dec. 880, 929 N.E.2d 531 (2010). If the allegations of the underlying complaint potentially fall within the policy's coverage, the insurer is obligated to defend the insured even if the allegations of the underlying lawsuit are groundless or false. *Id.*

¶ 19 Tony's has the burden of demonstrating that the facts alleged in the underlying Act complaint potentially fall within coverage of the policies at issue. See *Addison Insurance Co. v. Fay*, 232 Ill. 2d 446, 453, 328 Ill.Dec. 858, 905 N.E.2d 747 (2009).

¶ 20 The underlying Act complaint alleges that Tony's required Figueroa and other employees to scan their fingerprints into a database maintained by Kronos and to use Kronos's fingerprint recognition software to clock in and out of work. The complaint alleges that Tony's violated the Act by failing to (1) inform employees of the purpose and length of time for which their biometric data was being collected, stored, used, and disseminated, (2) publish a retention schedule for the permanent deletion of employees' biometric data, and (3) obtain releases from employees authorizing the collection, storage, usage, and dissemination of their biometric data. The complaint alleges that Tony's "improperly disclose[d] [its] employees' biometric data to at least one third-party, Kronos, and likely others," who are "currently unknown." The complaint alleges that Tony's violated subsections (a), (b), and (d) of section 15 of the Act (740 ILCS 14/15(a), (b), (d) (West 2018)) for, respectively, failing to publish a schedule for the deletion of biometric data, failing to obtain employees' written consent to collect their biometric data, and disclosing biometric data without employees' consent.

¶ 21 The insurance policy at issue provides coverage for losses incurred by Tony's resulting from "a data breach, security failure, or extortion threat." "[D]ata breach" means "the acquisition, access, or disclosure of personally identifiable information or confidential corporate information by a person or entity, or in a manner, that is unauthorized by [Tony's]." "[S]ecurity failure" means "any failure by [Tony's] or by others on [Tony's] behalf (including [Tony's] subcontractors, outsourcers, or independent contractors) in securing [Tony's] computer system." "[E]xtortion threat" means "a threat from a third-party to commit an intentional attack against [Tony's] website or computer systems or publicly disclose confidential corporate information or personally identifiable information misappropriated from [Tony's] if money, securities, or other property of value is not paid."

¶ 22 We find that the allegations of the underlying Act lawsuit do not even potentially fall within the policy's coverage. The policy provides coverage for Tony's losses resulting from a *data breach* or *security failure*.[4] The definitions of data breach and security failure do not include Tony's alleged violations of the Act via its own collection, use, storage, or dissemination of employees' biometric data. A data breach requires access to employee data that is *unauthorized* by Tony's. The underlying Act lawsuit does not allege that anyone obtained Tony's employees' biometric data without Tony's authorization. On the contrary, the underlying lawsuit alleges that Tony's (and Kronos, with Tony's authorization) collected, stored, used, and disseminated employees' biometric data. There is no allegation that Tony did not authorize these actions.

4 Tony's does not appear to contend that the allegations of the underlying Act lawsuit fall under the definition of "extortion threat."

***5** ¶ 23 Furthermore, the underlying Act lawsuit does not allege that Tony's or Kronos failed to secure their computer systems. In fact, the amended complaint says nothing at all about the security of Tony's or Kronos' computer systems.

¶ 24 *Remprex, LLC v. Certain Underwriters at Lloyd's London*, 2023 IL App (1st) 211097, 471 Ill.Dec. 141, 228 N.E.3d 321, guides our reasoning. That case involved a dispute over whether Remprex had insurance coverage for an Act class action alleging that Remprex and another transportation company collected truck drivers' fingerprint biometric data and shared it with each other without the drivers' permission. *Id.* ¶¶ 3, 9. This court found that Lloyd's had no duty to defend Remprex in the underlying Act lawsuit. *Id.* ¶ 78. The court explained the "data breach" coverage provision of the insurance policy at issue applied to "third-party breaches of [Remprex's] computer systems that in turn expose[d] the stored personal information to unauthorized persons." *Id.* ¶¶ 76, 78. However, the underlying

Act complaint "contained no allegations that an unauthorized third party accessed individuals' personal information and shared it with the public; instead, it merely alleged that the named parties engaged in the unauthorized collection of their personal information without their consent, which in turn is a violation of [the Act]." *Id.* ¶ 78. That scenario is essentially the same as this case. So, like the court in *Remprex*, we find that Lloyd's has no duty to defend Tony's in the underlying Act class action. See *id.*

¶ 25 Additionally, Lloyd's has no duty to defend Tony's because the policy specifically excludes from coverage allegations like those of the underlying Act lawsuit. The pertinent exclusion provides:

> "This policy does not apply to and [Lloyd's] will have no obligation to pay any loss, damages, claim expenses, or other amounts:
>
> 1. based upon or arising out of any actual or alleged:
>
> a. collection of information by [Tony's] (or others on [Tony's] behalf) without the knowledge or permission of the persons to whom such information relates; however, this exclusion will not apply if no board member, trustee, director, or officers (or equivalent position) of [Tony's] knew or had reason to know of such conduct; or
>
> b. use of personally identifiable information by [Tony's] (or others on [Tony's] behalf) in violation of law."

This language precisely describes the allegations of the underlying Act lawsuit and excludes them from coverage.

¶ 26 We acknowledge that neither the parties nor the circuit court addressed this exclusion. Generally, a reviewing court should not search the record for unargued and unbriefed reasons to reverse the circuit court's judgment. *People v. Givens*, 237 Ill. 2d 311, 323, 343 Ill.Dec. 146, 934 N.E.2d 470 (2010). However, that rule is relaxed when a reviewing court considers exclusionary language in an insurance policy because we review the interpretation of an insurance policy *de novo* and must consider the policy as a whole. *Landmark American Insurance Co. v. NIP Group, Inc.*, 2011 IL App (1st) 101155, ¶¶ 76-77, 356 Ill.Dec. 877, 962 N.E.2d 562. Moreover, we do "not lack authority to address unbriefed issues and may do so in the appropriate case, *i.e.*, when a clear and obvious error exists in the trial court proceedings." *Givens*, 237 Ill. 2d at 325, 343 Ill.Dec. 146, 934 N.E.2d 470. The parties' failure to bring an exclusion provision that clearly applies to this case to the circuit court's attention presents a scenario in which a "clear and obvious error" compels our independent consideration.

***6** ¶ 27 Tony's argues that the allegations of the underlying Act lawsuit potentially fall within the definition of "security failure" or "data breach" because, although Tony's authorized Kronos to access and store employees' biometric data, Tony's did not authorize Kronos to access or store that data in a non-Act-compliant manner. Tony's implies that Kronos committed a "security failure" that resulted in the disclosure of Tony's employees' biometric data to unknown third parties, *i.e.*, a "data breach." We disagree. The underlying Act complaint contains no allegations regarding the security of Tony's or Kronos's computer systems, and Figueroa does not allege that Kronos did anything with biometric data that was not authorized by Tony's.

¶ 28 Furthermore, the underlying complaint concedes that Figueroa and other "employees have no idea whether [Tony's] sells, discloses, re-discloses, or otherwise disseminates their biometric data." The complaint claims that "*if* a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed —like in the recent Google+, Equifax, Uber, Facebook/ Cambridge Analytica and Marriot data breaches or misuses —employees have no means by which to prevent" misuse of their biometric data. (Emphasis added.) The complaint also references a 2015 data breach at the United States Office of Personnel Management and a 2018 breach of an Indian biometric database called Aadhaar. These incidents may be examples of the type of data breaches that would qualify for coverage under the policy at issue, but none of them involves Tony's. Similarly, the complaint claims that Tony's Act violations "have raised a material *risk* that [Figueroa's] and other similarly-situated individuals' biometric data *will be* unlawfully accessed by third parties." (Emphasis added.) That statement presents a hypothetical scenario; it is not an allegation that such a breach has occurred.

¶ 29 Altogether, the underlying Act lawsuit describes Tony's and Kronos collecting, storing, using, and possibly disseminating Tony's employees' biometric data in ways that violate the Act. The insurance policy expressly excludes such allegations from coverage. The underlying Act lawsuit does *not* allege any sort of third-party access to Tony's employees' data that Tony's did not authorize, either due to computer security failures or for any other reason. That type of scenario is what the insurance policy covers. Accordingly, we find that the allegations of the underlying Act lawsuit do not even

potentially qualify for coverage; therefore, Lloyd's has no duty to defend Tony's.

¶ 30 Because we find that Lloyd's has no duty to defend Tony's in the underlying Act lawsuit, we need not address the parties' arguments regarding whether Tony's timely reported the Act lawsuit to Lloyd's. The allegations of the underlying Act lawsuit do not qualify for coverage regardless of whether Tony's timely reported that lawsuit to Lloyd's. Accordingly, we reverse the circuit court's grant of summary judgment in Tony's favor and remand with directions for the circuit court to enter summary judgment in favor of Lloyd's on the issue of the duty to defend. See *Pekin Insurance Co. v. United Contractors Midwest, Inc.*, 2013 IL App (3d) 120803, ¶ 35, 375 Ill.Dec. 232, 997 N.E.2d 235.

¶ 31 III. CONCLUSION

¶ 32 For the foregoing reasons, we reverse the circuit court's grant of summary judgment in Tony's favor and remand with directions for the circuit court to enter summary judgment in Lloyd's favor on the issue of the duty to defend.

¶ 33 Reversed; cause remanded with directions.

Justice D.B. Walker concurred in the judgment and opinion.

Justice Reyes dissented, with opinion.

¶ 34 JUSTICE REYES, dissenting:
¶ 35 I disagree with the majority's decision to reverse the grant of summary judgment in favor of Tony's and to direct the circuit court to enter summary judgment in favor of Lloyd's.

***7** ¶ 36 The duty to defend is a fundamental obligation of an insurer. *Employers Insurance of Wausau v. Ehlco Liquidating Trust*, 186 Ill. 2d 127, 151, 237 Ill.Dec. 82, 708 N.E.2d 1122 (1999). "An insurer may not justifiably refuse to defend an action against its insured unless it is clear from the face of the underlying complaint that the allegations set forth in that complaint fail to state facts that bring the case within or potentially within the insured's policy coverage." *General Agents Insurance Co. of America, Inc. v. Midwest Sporting Goods Co.*, 215 Ill. 2d 146, 154, 293 Ill.Dec. 594, 828 N.E.2d 1092 (2005). The allegations of the complaint should be liberally construed in favor of the insured, and the duty to defend exists even if the allegations are groundless, fraudulent, or false. *Acuity v. M/I Homes of Chicago, LLC*, 2023 IL 129087, ¶¶ 28-29, 473 Ill.Dec. 486, 234 N.E.3d 97.

¶ 37 In this case, I am unpersuaded by the majority's finding that the allegations of the underlying Biometric Information Privacy Act (740 ILCS 14/1 *et seq.* (West 2018)) complaint do not even potentially fall within the policy coverage. Tony's contracted with Kronos to manage the employees' biometric information. A plausible inference is that Tony's expected Kronos to manage the biometric information in a manner compliant with applicable law. To the extent that the operative complaint alleges unlawful disclosures of such information, those allegations potentially fall within the definition of a "data breach" or a "security failure," as defined in the policy. Furthermore, I consider the majority's analysis of a policy exclusion that was not raised by the parties to be unnecessary and possibly improper, irrespective of our *de novo* standard of review. See *Commonwealth Edison Co. v. Illinois Commerce Comm'n*, 2016 IL 118129, ¶ 10, 402 Ill.Dec. 36, 51 N.E.3d 788 (noting that reviewing courts generally do not render advisory opinions).

¶ 38 When the underlying complaint against the insured alleges facts within or potentially within the scope of the policy coverage, the insurer taking the position that the complaint is not covered by the policy must either defend its insured under a reservation of rights or seek a declaratory judgment that no coverage exists. *State Farm Fire & Casualty Co. v. Martin*, 186 Ill. 2d 367, 371, 238 Ill.Dec. 126, 710 N.E.2d 1228 (1999). Based on its failure to take either of these steps, I agree with the circuit court's conclusion that Lloyd's is estopped from asserting a late-notice defense (or any other defense). Therefore, I respectfully dissent.

All Citations

--- N.E.3d ----, 2024 IL App (1st) 231712, 2024 WL 4128238

HUNTON
ANDREWS KURTH

Hunton Insurance Recovery Blog

UPDATES, ANALYSIS AND BREAKING NEWS FOR COMMERCIAL POLICYHOLDERS

SEC Cyber Disclosure Charges Highlight Role of D&O Insurance to Mitigate Cyber Risks

3 Minute Read
| October 30, 2024

By Andrea DeField, Geoffrey B. Fehling and Evan Warshauer
Categories: Cyber, D&O

Following an investigation involving public companies potentially impacted by the 2020 SolarWinds software compromise, the US Securities and Exchange Commission recently charged several companies with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC's enforcement is the latest example of "cyber as a D&O risk," underscoring the importance of maintaining robust directors and officers (D&O) liability coverage, along with cyber insurance, as part of a comprehensive liability insurance program designed to respond to cyber incidents.

Background

On October 22, 2024, the SEC charged four current and former public companies with making materially misleading disclosures regarding cybersecurity risks and intrusions related to the 2020 SolarWinds Orion hack. The SEC specifically found that each company learned in either 2020 or 2021 that the threat actor behind the SolarWinds Orion hack had accessed their systems without authorization, but that the companies negligently minimized the cybersecurity incident in public disclosures. The companies did so, the SEC contends, by

framing the relevant cybersecurity risk factors hypothetically or generically when they knew the warned of risks had already materialized.

The SEC concluded that each company had violated certain provisions of the Securities Act of 1933, the Securities Exchange Act of 1934 and related rules. Without admitting or denying the SEC's findings, each company agreed to cease and desist from future violations of the cited provisions and to pay civil penalties ranging from $990,000 to $4 million.

Discussion

The recent SEC charges continue the trend of increased federal scrutiny by the SEC, DOJ and FTC following cybersecurity incidents. Individual directors and officers may also face personal liability, as regulators have targeted not just companies, but also individuals, in the wake of major cyber attacks. In 2022, for example, Uber's former Chief Information Security Officer was criminally prosecuted and convicted by the FTC for failing to disclose a data breach during an ongoing investigation. More recently, the SEC's far-reaching case against SolarWinds and its CISO was largely truncated in a highly-anticipated ruling earlier this year, but certain charges against the CISO were allowed to proceed.

Cyber insurance remains critical for protecting all companies from the fallout of a cyber incident—regardless of their particular industry or trade. But with the staggering cost of cybersecurity events ($9.48 million on average in the US), cyber insurance limits are often quickly eroded, if not exhausted entirely, in the immediate aftermath of a cyber event. Those risks, combined with continued increase in government investigations, enforcement actions and follow-on civil and criminal claims against both companies and individuals, make complementary D&O coverage even more critical to fill any gaps and respond to traditional D&O exposures that may arise following a cybersecurity incident.

From building a comprehensive cyber and D&O insurance program to ensuring that in-house cybersecurity professionals like CISOs do not fall through the cracks in traditional policies, we have previously outlined common pitfalls and best practices to consider in addressing these risks. Being proactive and consulting with insurance brokers, outside coverage counsel and other risk professionals at the time policies are negotiated, renewed and placed can help avoid unexpected denials and maximize the chance of recovery in the event of a claim.
Tags: Cyber, D&O, Government Investigations

Andrea DeField

Partner
+1 305 810 2465

Email | vCard | Bio | Posts

Andrea helps companies navigate disasters and swiftly recover insurance funds to restore operations with minimal impact to the bottom line. She leads the Firm's cyber insurance practice.

With an undergraduate degree focused on ...

Geoffrey B. Fehling

Partner
+1 617 648 2806

Email | vCard | Bio | Posts

Geoff works closely with corporate policyholders and their directors and officers to resolve high-stakes insurance disputes.

As a partner in Hunton's top-ranked insurance coverage practice, he has recovered hundreds of ...

Evan Warshauer

Associate
+1 202 419 2117

Email | vCard | Bio | Posts

Evan advises policyholders in insurance coverage matters and complex insurance litigation. As a member of the firm's nationwide insurance coverage team, Evan represents commercial policyholders in a range of matters ...

HUNTON
ANDREWS KURTH

Hunton Insurance Recovery Blog

UPDATES, ANALYSIS AND BREAKING NEWS FOR COMMERCIAL POLICYHOLDERS

From Produce to Insurance Coverage: What Businesses Concerned About Illinois Biometric Information Privacy Act (BIPA) Risks Can Learn From *Tony's Finer Foods*

5 Minute Read

| October 3, 2024

By Andrea DeField, Rachel E. Hudgins and Alex D. Pappas
Categories: Commercial General Liability, Cyber

Just two months ago, Illinois Governor J. B. Pritzker signed significant amendments to the Illinois Biometric Information Privacy Act (BIPA). While the amendments limit businesses' exposure to BIPA-related damages, significant BIPA exposures still persist. Given these continuing exposures, businesses should consider the protections that insurance can offer. The Illinois Appellate Court's September 2024 decision in *Tony's Finer Foods Enterprises v. Certain Underwriters at Lloyd's*, 2024 IL App (1st) 231712 offers concrete guidance for businesses thinking about doing just that.

Background

A plaintiff filed a putative class action alleging that grocer Tony's Finer Foods violated BIPA by requiring employees to scan their fingerprints to clock in and out of work. The fingerprints, which are biometric information under BIPA, were allegedly maintained in a database by third-party Kronos. Tony's tendered the lawsuit to its cyber insurer Lloyd's. Lloyd's denied coverage and litigation ensued.

Lloyd's defended its coverage denial by arguing that the lawsuit did not fall within the cyber policy's insuring agreement. The cyber policy extended coverage for Tony's "loss" "resulting from" a "data breach" or a "security failure." The policy defined "data breach," in pertinent part, to mean "the acquisition . . . of personally identifiable information . . . in a manner, that is unauthorized by" Tony's. The policy defined "security failure" to mean any failure by Tony's or its contractors in securing Tony's computer systems.

Tony's argued that the underlying BIPA lawsuit fit within the definitions of "data breach" and "security failure." According to Tony's, the underlying lawsuits alleged that data was disclosed in a manner unauthorized by Tony's in that Tony's did not authorize Kronos to access or store the biometric data in a BIPA non-compliant manner. In a dissenting opinion, Justice Reyes credited Tony's argument in finding that Lloyd's had a duty to defend. According to Justice Reyes, a "plausible inference is that Tony's expected Kronos to manage the biometric information in a manner compliant with applicable law."

The majority disagreed. It reasoned that the underlying lawsuit did not "allege any sort of third-party access to Tony's employees' data that Tony's did not authorize, either due to computer security failures or for any other reason," which is the only scenario that, according to the Court, this cyber insurance was meant to cover. The majority also held that an exclusion neither the parties nor the circuit court raised independently barred coverage.

The Cyber Insurance Market Response to *Tony's* and Other BIPA Risks

The cyber insurance market has been grappling with how to address BIPA and other biometric liabilities and exposures for some time. Some insurers have added express biometric data exclusions to all of their policies to avoid BIPA risks. Others have focused more on biometric exposures in underwriting, only adding potentially applicable exclusions where the risk profile for that insured is high. Other insurers have not added exclusions, instead relying on existing wrongful collection of data exclusions in their policies to capture this risk and/or relying on narrow insuring agreements that would not encompass most BIPA claims.

Practice Pointers

While the *Tony's* court found for the insurer and denied coverage to a policyholder, there are still avenues for policyholders seeking insurance coverage for BIPA claims. After *Tony's*, businesses seeking insurance coverage for BIPA claims should consider the following:

1. **Choice of Law**: Because BIPA is an Illinois statute, most case law interpreting the applicability of insurance to BIPA claims has happened to also arise in Illinois. But not all insurance policies are subject to Illinois law – most are not. Indeed, they are likely to be governed by the laws of other states such as the state where a given business is incorporated or headquartered. And when the law of other states applies, policyholders can litigate these issues as matters of first impression, including with citation to and support from Justice Reyes' dissenting opinion.
2. **Policy Language**: Insurance policy language—especially cyber insurance policy language—is not standardized and can vary substantially from policy to policy. When the policy language is different, *Tony's* will not control a court's disposition of whether cyber insurance is available for a specific BIPA claim, even for other policyholders bound by Illinois law. Policyholders should look for broad insuring agreements around privacy risks and try to avoid—or at least narrow—overbroad "wrongful collection" and biometric data exclusions.
3. **Other Lines of Coverage**: While cyber insurance is a potential source for insurance coverage for BIPA claims, so too are commercial general liability (CGL) and errors & omissions (E&O) insurance policies. So businesses should be sure to notify insurers other than their cyber insurer. Indeed, relative to the same underlying lawsuit at issue in *Tony's*, a federal court found that Tony's *was* entitled to coverage under a CGL policy. *See Cont'l W. Ins. Co. v. Tony's Finer Foods Enterprises, Inc.*, 2023 WL 4351469 (N.D. Ill. July 5, 2023).

Tony's is a timely reminder to policyholders to consider their coverage for BIPA claims before a lawsuit is filed. As always, consultation with experienced coverage counsel can be essential to ensure that your insurance program is prepared to respond when a BIPA claim arises.
Tags: Biometric Information, Biometric Information Privacy Act (BIPA), CGL, Cyber

Andrea DeField
Partner
+1 305 810 2465

Email | vCard | Bio | Posts

Andrea helps companies navigate disasters and swiftly recover insurance funds to restore operations with minimal impact to the bottom line. She leads the Firm's cyber insurance practice.

With an undergraduate degree focused on …

Rachel E. Hudgins

Counsel

+1 404 888 4110

Email | vCard | Bio | Posts

Rachel has litigated hundreds of insurance coverage and bad faith claims in state and federal courts across the country and U.S. territories brought under a spectrum of insurance policies issued to individuals, public and private …

Alex D. Pappas

Associate

+1 202 955 1887

Email | vCard | Bio | Posts

Alex counsels clients on all aspects of insurance coverage. He guides them in obtaining appropriate coverage and resolving disputes over coverage, including in litigation and arbitration.

Before joining Hunton Andrews Kurth …
