2022 Product Liability & Complex Torts Seminar

June 1-3, 2022

COVID SCHOOLED US:

Learned and New Strategies Devised from Managing Through the Pandemic

Steve Hamilton
Moderator
HALL & EVANS LLC
Denver, Colorado
hamiltons@hallevans.com

INTRODUCTION – WHERE ARE WE NOW WITH COVID-19?

This seminar was going to occur in October 2021. The Pandemic got worse again and so our Practice Group canceled the seminar and rescheduled it for the current planned dates. I had written the following introduction for the October 2021 seminar date:

> As I write this in August 2021, the status of Covid and how businesses are handling it is still very much unresolved. Only a couple months ago, it appeared the Pandemic was going to be completely over, at least in the United States. Three vaccines had been approved for emergency use by the FDA and were mostly available in the United States. Moreover, all Covid indicators had hit low points since the Pandemic's beginning.[1]
>
> But then the highly contagious Delta variant started spreading like a California wildfire, mainly through the unvaccinated, but infecting some vaccinated people and making some of them sick as well. On July 27, 2021, the Centers for Disease Control recommended that everyone in areas with high COVID-19 infection rates wear masks in public indoor spaces, regardless of vaccination status. Thus, the bottom line is that we have not yet completely emerged from the Pandemic and so, while we can take some educated guesses as to what strategies may remain after the Pandemic, they are only educated guesses.

I am now writing a supplement in March 2022 for the seminar in June 2022. The Delta variant came and went and then the Omicron variant came and went. As I'm writing this, a subvariant of Omicron, BA.2, is emerging. The U.S. seems to be generally over caring about Covid, although there are no doubt still concerned citizens among us. Russia's invasion of Ukraine started in late February and that has dominated the news since then. Thus, this topic, although titled "Covid Schooled Us" really involves businesses' reactions to Covid and other crises.

All that said, I think when you are reading this, presumably around June 2022, we will be in a good position to discuss this topic. Regardless of whether Russia is still invading Ukraine or the aftermath of that invasion is occurring and regardless of whether a new Covid variant is infecting the world population, we will have been living with these crises long enough to have a good idea how businesses are reacting to them and preparing for the next one.

INTRODUCTION – WHAT HAS CHANGED DUE TO THE PANDEMIC AND OTHER CRISES?

Our panelists for the General Session on the titled topic, which include Jolene Wall with REI, Nicole Brunson with Arrival, and Chris Schilder with Safway, identified some areas within the business risk segment that are likely going to be affected and changed because of the Pandemic and other crises.

- Business Continuity Planning – how do businesses change their plans to withstand crises in the aftermath of Covid?
- Environmental, Social, and Corporate Governance (ESG) – how has Covid, the social movement, and the Ukraine invasion changed businesses' collective conscientiousness for social and environmental factors?
- Employment Issues
    - Hybrid Work Environment – how has Covid changed the work environment in businesses?
    - Hiring of New Employees – has Covid changed hiring policies and candidate pools?
    - Unions – are unions forming or getting bolder?

[1] The World Health Organization declared the COVID-19 outbreak a Pandemic on March 11, 2020.

- Cybersecurity – cyber crime is a major concern recently, not necessarily due to Covid. How are businesses preparing for it?
- Litigation Issues – how will businesses change litigation practices including attorney travel, deposition preparation and recording, and outside counsel requirements?

Let's look at each of these in more depth.

A. Business Continuity Planning

In a survey conducted by insurance broker Aon, "82% of respondents said that prior to COVID-19, a pandemic or other major health crisis was not a top 10 risk on their organization's risk register; their Enterprise Risk Management (ERM) strategy and management failed to pick up the threat of the pandemic. And when it hit, their risk infrastructure struggled to cope with the initial response."[2]

The Aon Report goes on to say: "Going forward, risk and business leaders must reprioritize risk—broadening their perspective and evaluating major shocks, not just anticipated losses, and elevating risk managers to an enterprise-level strategic role. By doing so, they will also be able to redefine resilience. Together, these are the post-COVID-19 imperatives required to reshape businesses into a more future-ready posture."[3]

The Aon survey revealed that 79% of businesses said they would be more dependent on ERM to reduce volatility in performance and 65% said they would look at insurance solutions. In addition, all sectors agreed that protecting people was the top priority. The Aon Report concludes that businesses will need to rethink their ERM, build a more resilient workforce, and look to insurance solutions.[4]

Because of these concerns, businesses need to be better prepared through business continuity planning. "Generally speaking, business continuity plans involve an enterprise-level, coordinated effort to safeguard corporate equities, including data and critical infrastructure, from all threats—both man-made and natural. In theory, a well-designed and practiced plan would allow the affected business or agency to reestablish critical or core operations within a maximum of 72 hours after the onset of the crisis scenario. Business continuity planning requires dedicated personnel and meticulous planning, employee awareness, tabletop scenarios, and coordination with local first responders and emergency services personnel. It cannot be done at the last minute or on the fly, or the entity risks cascading into a state of general chaos during an incident." [5]

"In a private enterprise scenario, your core functions must be identified so that your continuity plan ensures their partial operation within the shortest amount of time possible. To accomplish this, it is essential to conduct a business impact assessment, followed up by detailed and extensive planning and response protocols that are disseminated throughout your workforce."[6]

Stephen Cocco, a consultant with Asis International, a security management company, suggests that you ask

---

[2] https://www.aon.com/reprioritizing-enterprise-risk-management-resilience-and-insurance-covid19/index.html
[3] *Id.*
[4] *Id.*
[5] Asis International, "Updating Business Continuity Basics After COVID-19," Stephen Cocco, 17 May 2021: https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2021/updating-business-continuity-basics-after-covid-19/

[6] *Id.*

yourself what your business's core functions are. He states, as examples:

"Core functions for a hotel or cruise ship hit by widespread food poisoning, for example, would include prioritizing the safety and security of guests, the bulk of whom would be confined to their rooms. Food service would be limited to delivery of pre-packaged meals. For a distributor of business supplies, core functions might include securely storing client billing data, order history, and other details. Securing current stock on hand might be deemed non-essential for the duration of the crisis."[7]

Other questions include:

- What is the status of your main facility, warehouse, or office?
- Are your personnel able to safely report to work, at least on a part-time or shift basis?
- Where is management, and who is in charge?
- What are some elements of your continuity planning that might need to be altered in order to address a pandemic as opposed to reestablishing operations after the primary worksite has been destroyed or rendered inaccessible?[8]
- Who is in your supply chain and is your supply chain diversified?
- How might significant inflation affect your business?
- How will government instability in certain countries affect your business?

  These issues all need to be revisited in the wake of the Pandemic to allow your business to be prepare for the next pandemic or other interruption event.

B. Environmental, Social, and Corporate Governance (ESG)

In an article for its clients, consultant Weber Shandwick stated:

"Beyond upending economies and societies and disrupting business and supply chains, the pandemic also reinforced global economic and societal gaps and disparities – prompting a new sense of urgency to build more inclusive and fairer economies.

Governments, businesses, investors and civil society are now calling for more accountability to address key challenges for society and the planet. Already this year, there have been significant developments on the ESG policy front:

- The Group of Seven (G7) endorsed the Task Force on Climate-related Financial Disclosures (TCFD) and signaled support for making climate risk disclosure mandatory.
- The Group of Twenty (G20) announced backing for a new International Sustainability Standards Board (ISSB) to create a climate disclosure standard by the middle of next year.
- The European Union is moving forward with an overhaul of sustainable finance policy and larger climate initiatives, with its 'Fit for 55" legislative package this week.

And beyond climate, regulators are looking at broader social and governance disclosure to address diversity,

[7] *Id.*
[8] *Id.*

equity and inclusion (DE&I) and social justice issues." [9]

As an example of ESG disclosures, "Insurance broker Marsh recently announced the launch of its Environmental, Social, and Governance (ESG) Risk Rating, an assessment tool that can measure an organization's ESG performance, enabling them to improve their ESG risks, and gain access to additional insurance market capacity.

Measured against more than 10 internationally recognized standards and frameworks published by leading organizations – including the Global Reporting Initiative, Sustainability Accounting Standards Board, Task Force on Climate-related Financial Disclosures, and the World Economic Forum – the ESG Risk Rating scores a client's performance across 18 ESG themes. On completion of the free assessment, the organization receives an overall ESG risk score, as well as a rating for each ESG component."[10]

And on March 21, 2022, the U.S. Securities and Exchange Commission (SEC) "unveiled a landmark proposal requiring U.S.-listed companies to disclose their climate-related risks and greenhouse gas emissions, part of a push by President Joe Biden's administration to address financial risks created by global rising temperatures.

The long-awaited draft rule should help investors better understand how climate change will affect the companies they invest in, but it is set to increase the reporting burden for Corporate America.

Among its key requirements: companies must disclose their own direct and indirect greenhouse gas emissions, known as Scope 1 and 2 emissions, respectively, as well as those generated by suppliers and partners, known as Scope 3 emissions, if material." [11]

The Weber Shandwick article concludes:

"In addition to developing more robust ESG strategies and communications programs, companies must now navigate new pressures for transparency on ESG factors and performance. As the policy landscape evolves, companies must prepare now.

Here is some practical guidance for corporate leaders:

- TRACK ESG REGULATION: Put processes in place to carefully track and evaluate the proposed legislation and regulatory developments in markets such as the EU, UK, U.S., India, China and other regions that impact your operations.
- ASSESS DISCLOSURE RISK: Companies should review their current processes, data and controls related to ESG disclosures and ensure these are accurate, up to date and reliable. Companies should also identify policy areas that will expose risk or gaps in existing transparency policies and proactively update those policies and practices ahead of policy adoption.
- EVOLVE ESG GOALS: Companies should ensure their portfolio of ESG activities and goals are both aligned with stakeholder expectations for transparency and anticipate new reporting mandates. All companies should set tangible and timebound ESG goals – ideally evidence-based – and report on impact at least annually, using commonly accepted frameworks understood by investors and other stakeholders.

---

[9] Weber Shandwick, Client Advisory, "ESG in a Post-Disclosure World: A Global Policy Guide for Business," July 2021: https://www.webershandwick.com/news/esg-disclosure-post-covid-world/

[10] "Marsh Launches ESG Risk Rating to Assess Companies' ESG Performance," *Insurance Journal*, March 21, 2022.

[11] Katanga Johnson and editing by Michelle Price, David Gregorio and Matthew Lewis, "U.S. SEC Unveils Landmark Climate Change Risk Disclosure Rule," *Insurance Journal*, March 21, 2022.

- ADVOCATE WITH STAKEHOLDERS: The business sector has an opportunity to help shape the ESG disclosure policy landscape by engaging with key stakeholders – including policymakers and investors. Articulating a clear agenda for ESG transparency and the role business can and should play is an important component of the policy development process. The business sector can demonstrate alignment with global collaborative frameworks such as the Paris Climate Agreement and commit to transparent communication about progress against them.

This is a time for boards, CEOs and executive leadership to monitor the emerging policy landscape and prepare for a new era of ESG action."[12]

While ESG is not specific to the Pandemic, ESG has certainly become more prevalent since the Pandemic began and must be addressed.

C. Employment Issues

As noted above, workforce is the number one priority for employers after the Pandemic. The three most discussed issues are creating a hybrid work environment, how hiring employees has changed, and the effects on unions.

1. Hybrid Work Environment

Hybrid work environment is simply allowing employees to work remotely some or all the time. In one study done by workplace platform software company Envoy and Wakefield Research in March 2021, nearly half of all employees stated they would look for another job if their employers did not offer a hybrid work model.[13]

Employees want a hybrid work model because (1) they can work when they are most effective, (2) they can maintain a better work-life balance, (3) the commute is eliminated, (4) exposure to illness is reduced, and (5) they can live where they want to live or where they can get better value.

Employers like the hybrid work model because they can reduce office costs and they can hire employees around the world.

But there are downsides as well: (1) collegiality is diminished, (2) company culture is harder to achieve, (3) loyalty is not fostered, (4) cyber security is more easily compromised, and (5) it is more difficult to monitor performance.

Because of the demand for it, companies need to allow for hybrid work models, but they need to address the downsides as best as possible. The downsides can be addressed through virtual meetings, regular in-office meetings (to the extent possible), and company events. And performance could be tracked through an employee logging into the company system. Logging into the company system can help with cyber security also because the employee will have to log into a protective VPN to access the company system.

Hybrid work models are here to stay, so companies need to determine the best way to incorporate them.

2. Hiring Employees

The biggest difference between hiring employees pre-Pandemic and post-Pandemic is in a company's ability to

[12] *Supra* FN 9.
[13] Tiffany Fowell, Envoy, "Hybrid Work: What is Hybrid Work and Why Do Employees Want It?" July 7, 2021: https://envoy.com/blog/what-is-a-hybrid-work-model/

offer the hybrid work model or remote work model. Many workers simply are not going to accept a job that does not offer a hybrid work model. As part of that offer, decisions need to be made as to who is going to pay for the technology the employee needs at his or her home office to be able to work remotely. The company is saving on the office space, so it many instances, it could cover similar costs for a remote-working employee.

Remote working involves an employee logging into the company's system remotely. Thus, it is important for an employee to have the technological knowhow to use the system remotely. Moreover, the employee will need to get cyber security training to make sure he or she does not misuse the system while working remotely allowing a hacker to steal from or infect the company's technology system. Employers will need to make sure employees wanting to work remotely can handle these requirements.

With the ability to allow an employee to work from anywhere, the candidate pool has dramatically increased. A candidate living in Montana or the U.S. Virgin Islands who never would have considered a job in Los Angeles, for example, may now be able to do that same job from Montana or the Islands. The employer now has access to more quality candidates and the employee has access to more quality jobs. It's a win-win.

Overall, the hiring process will not necessarily change, but the offer of a hybrid work model or remote work model and ensuring the employee can responsibly handle the model have become critical hiring factors.

3. Unions

"In the wake of the Covid-19 pandemic, unions are finding they suddenly have the upper hand—or at least, more solid footing—when it comes to negotiating wages and benefits, spurring a flurry of new picket lines. Nearly 40 workplaces across the nation have gone on strike since Aug. 1, [2021] according to Bloomberg Law's database of work stoppages, almost double the number during the same period last year."[14]

"But now employees, trying to reclaim what they gave up before, have been emboldened by a series of related events: soaring company profits, a renewed respect for essential workers and rekindled political will in Washington. Plus there's the hard truth of today's labor market: Companies in many industries are finding employees downright impossible to replace."[15]

Businesses will need to address the employees' requests to keep a union from starting in the first instance or to keep the current union appeased, something it may have been able to avoid before the Pandemic.

D. Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

The Cybersecurity and Infrastructure Security Agency (CISA) was created in 2018 to defend critical infrastructure against threats. CISA establishes a voluntary method for sharing cyberthreat intelligence between private businesses and government agencies, with the aim of helping organizations quickly identify and mitigate potential

[14] Ian Kullgren, Brian Eckhouse, and Deena Shanker, "U.S. Labor Unions Are Having a Moment," *Time*, October 17, 2021.
[15] *Id.*

cyber incursions. Under CISA, the Department of Homeland Security (DHS) will receive and store cyberthreat indicators—including samples of malicious computer code—from participating organizations and use that information to develop recommended defensive measures. CISA authorizes individuals or organizations to share cyberthreat indicator information after removal of all personal information not directly related to the threat.

CISA works with businesses, communities, and government at every level to help make the nation's critical infrastructure more resilient to cyber and physical threats. Everyone has a role securing the Nation's critical infrastructure.

But CISA is having difficulty identifying the next risks while keeping up with the attacks that have occurred. "Staffers are worn out, money is tight and the Cybersecurity and Infrastructure Security Agency is struggling to keep up with multiple competing crises, including the recently uncovered intrusions blamed on Russia and China, according to interviews with 15 people familiar with CISA's work. Among them are four current employees and five former agency officials.

'CISA is overworked, understaffed and in one sense fighting half-blindfolded,' said Andy Keiser, a former House Intelligence Committee staffer who is in touch with current and former CISA officials.

Many of those who track the nation's cyber defenses say they're worried that CISA — with roughly 2,000 employees — is so consumed with recovering from the existing breaches that it's too stretched to prepare for the next attack, potentially making future breaches more widespread or more damaging to U.S. economic and national security."[16]

Regardless of what help is out there, all businesses can help themselves through cybersecurity best practices:

a. Train your employees

   i. Employees and emails are a leading cause of data breaches for small businesses because they are a direct path into your systems. Training employees on basic internet best practices can go a long way in preventing cyber-attacks. The Department of Homeland Security's "Stop.Think.Connect" campaign offers training and other materials.

   ii. Training topics to cover include:

   - Spotting a phishing email
   - Using good browsing practices
   - Avoiding suspicious downloads
   - Creating strong passwords
   - Protecting sensitive customer and vendor information

[16] Eric Geller, "America's digital defender is underfunded, outmatched and 'exhausted,'" *Politico*, March 31, 2021.

- Maintaining good cyber hygiene

b. Use antivirus software and keep it updated – Make sure each of your business's computers is equipped with antivirus software and antispyware and updated regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.

c. Secure your networks – Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router.

d. Use strong passwords – Using strong passwords is an easy way to improve your cybersecurity. Be sure to use different passwords for your different accounts. A strong password includes:

- 10 characters or more
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

e. Multifactor authentication – Multifactor authentication requires additional information (e.g., a security code sent to your phone) to log in. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

f. Back up your data – Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible, or at least weekly, and store the copies either offsite or on the cloud.

g. Secure payment processing – Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Isolate payment systems from other, less secure programs and do not use the same computer to process payments and surf the Internet.

h. Control physical access – Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them

> up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel."[17]

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider. Attached is a document from the Federal Trade Commission as to what a business should look for in cyber insurance.[18] While this document was created for small businesses, the tips are relevant for any size organization.

Cyber crimes are not going away anytime soon. Businesses need to be prepared to avoid losing data leading to costly lawsuits or being forced to pay to ransom to get control of their systems back.

E. Litigation Issues

Litigation is going to see changes from the Pandemic in areas such as travel for in-house attorneys and outside counsel. How depositions, trials, and hearings are conducted may also change. Finally, companies may ask outside counsel to consider these other options early.

One of the biggest changes in litigation is through videoconferencing use. The dramatic increase is well-depicted by looking at Zoom's stock price history. On January 3, 2020, Zoom's stock price was $67.28. On October 16, 2020, Zoom's stock price was $559.00! (As of this writing, it was $110.79 – it now has multiple competitors and videoconference use, while still widely used, has diminished from its peak.)

With everyone being told to stay home and with courthouses closing, everyone took to videoconferencing. It was a necessity during that time, but even as we return to open courthouses and travel, it appears videoconferencing is here to stay.

Videoconferencing can provide significant savings due to no travel costs and no travel-time fees. And of course, videoconferencing avoids exposure to contaminated people. Thus, some companies are now requiring their in-house counsel to justify attending a mediation in person or their outside counsel to justify attending depositions in person. Companies will likely still allow in-person attendance, but the attorney will need to provide reasons for the in-person attendance, e.g., where the witness is a key witness that would require a face-to-face question-and-answer session or where many exhibits are involved, which can be easier to manage when sitting in front of a witness.

Witnesses can now appear via videoconferencing for trial or hearings. Doing so saves costs, of course. In addition, it allows distant witnesses to attend live, albeit on a video screen. But live is better than a video-recorded deposition, which is the other typical alternative. Again, the company and outside counsel need to weigh the pros and cons and decide on a witness-by-witness basis what works better for the situation.

Videoconferencing requires good internet connections and a good location with proper lighting and sound. Those issues need to be considered whenever video conferencing is considered. For example, a terrible internet connection such that the witness is cutting in and out will negatively overshadow any cost savings from using

[17] https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
[18] Cyber Insurance FTC flyer, attached.

videoconferencing.

You also must be sure you know the rules on swearing in the witness and whether there will be any concerns with the testimony's admissibility.

The cost savings from videoconferencing is so significant that companies will likely demand that their outside counsel consider these issues and present options for litigation.

CONCLUSION

Covid did school us in that there were hundreds of thousands of lives lost and it seems almost everyone got sick in varying degrees of severity. It also destroyed many businesses that relied on in-person traffic.

Covid has also schooled us in teaching us how to be prepared for the next pandemic or crisis. It also schooled us in forcing us to adopt new methods. Some of these methods have proven to simply be better ways to conduct business or litigation and will continue even post-Covid.

Yes, Covid schooled us and, as with any horrible event, we need to learn from it and become better because of it.

CYBERSECURITY FOR
SMALL BUSINESS

CYBER INSURANCE

Recovering from a cyber attack can be costly.

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?

Make sure your policy includes coverage for:

- ☐ Data breaches (like incidents involving theft of personal information)
- ☐ Cyber attacks (like breaches of your network)
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Cyber attacks that occur anywhere in the world (not only in the United States)
- ☐ Terrorist acts

Also, consider whether your cyber insurance provider will:

- ☐ Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- ☐ Provide coverage in excess of any other applicable insurance you have
- ☐ Offer a breach hotline that's available every day of the year at all times

LEARN MORE AT:
FTC.gov/SmallBusiness

NAIC National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.

CYBERSECURITY FOR
SMALL BUSINESS

WHAT IS FIRST-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- ☐ Legal counsel to determine your notification and regulatory obligations
- ☐ Customer notification and call center services
- ☐ Crisis management and public relations
- ☐ Forensic services to investigate the breach
- ☐ Recovery and replacement of lost or stolen data
- ☐ Lost income due to business interruption
- ☐ Cyber extortion and fraud
- ☐ Fees, fines, and penalties related to the cyber incident

WHAT IS THIRD-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- ☐ Payments to consumers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages, and judgments
- ☐ Accounting costs

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness

LEARN MORE AT: FTC.gov/SmallBusiness

NAIC National Association of Insurance Commissioners

The FTC thanks the National Association of Insurance Commissioners (NAIC) for its role in developing this content.