Articles + Publications | February 9, 2026

‘FirstEnergy’ and Incident Response: Preserving Privilege in Cyber Investigations

WRITTEN BY

Sadia Mirza | Timothy J. St. George | Kaitlin J. Clemens

Investigations led by counsel, triggered by legal risk, and designed to elicit legal advice remain protected, even if their findings later inform business decisions. For cyber incidents, FirstEnergy outlines how to structure IR investigations to maximize privilege and work product protection while supporting an effective technical and business response.

The U.S. Court of Appeals for the Sixth Circuit’s decision in *In re FirstEnergy Corporation* (*FirstEnergy)*, is a roadmap for best practices in preserving attorney–client privilege and work product protection in cyber incident investigations, with direct implications for incident response (IR).

The question in *FirstEnergy* was whether a company that faces legal exposure and retains outside counsel for an internal investigation must turn over investigation materials to civil plaintiffs. The Sixth Circuit held no.

Investigations led by counsel, triggered by legal risk, and designed to elicit legal advice remain protected, even if their findings later inform business decisions. For cyber incidents, *FirstEnergy* outlines how to structure IR investigations to maximize privilege and work product protection while supporting an effective technical and business response.

BACKGROUND: THE FIRSTENERGY INVESTIGATION AND DELUGE OF LITIGATION

More than five years ago, FirstEnergy was drawn into a political corruption scandal involving an alleged bribery scheme with Larry Householder, then Speaker of the Ohio House of Representatives, to secure favorable legislation. In July 2020, the U.S. Department of Justice (DOJ) filed a criminal complaint against Householder and served subpoenas on FirstEnergy. When the complaint became public, FirstEnergy’s stock price fell sharply, and the company anticipated legal exposure, shareholder suits and regulatory proceedings.

The board formed a committee and retained Squire Patton Boggs, while the company retained Jones Day. Both firms investigated, assessed potential liability, advised on subpoenas and government inquiries, and recommended governance and compliance reforms.

The DOJ action triggered shareholder suits and investigations by regulators. In one securities case, shareholders

sought “all previously withheld documents” related to the investigations. A special master recommended, and the district court ordered, production of those materials, finding no privilege or work product protection. FirstEnergy sought relief, and the Sixth Circuit granted mandamus and vacated the order, clarifying when internal investigations are protected—and when they are not.

THE SIXTH CIRCUIT’S DECISION

The Sixth Circuit held that investigations by outside counsel, designed to assess legal exposure and provide advice, are classic attorney–client communications.

Investigations conducted “to secure legal advice” fall within the attorney–client privilege. The key question is whether the company sought legal advice, not whether the advice later informed business decisions. Using legal advice to guide business choices does not strip it of privilege.

Second, the court held that the investigation materials were protected work product because they were created “because of” actual and anticipated litigation and regulatory actions. Even where documents have both legal and business purposes, they can qualify as work product if reasonably anticipated litigation is a driving force behind their creation.

Third, sharing high?level conclusions or factual summaries with third parties (including auditors) does not automatically waive privilege or work product protection over underlying communications, analyses, or mental impressions. Disclosing factual findings is not the same as revealing counsel’s thought process.

Although *FirstEnergy* arose from a bribery and securities context, its reasoning maps well onto cyber incidents, where companies face immediate legal risk and must investigate quickly while communicating with regulators, insurers, auditors, and customers.

KEY LESSONS FROM ‘FIRSTENERGY’ FOR IR INVESTIGATIONS

Cyber incidents regularly result in regulatory investigations, class actions, contract and indemnity claims, and securities and disclosure issues. In that sense, they present the same kind of “very significant legal risk” that drove FirstEnergy’s response.

FirstEnergy shows that, if structured thoughtfully and properly, an IR investigation can be treated as a legal investigation: directed by counsel, initiated because of real or reasonably anticipated legal exposure, and therefore eligible for attorney–client privilege and work?product protection. *FirstEnergy*, however, does not guarantee this. Instead, it offers practical guidance on how to perform IR investigations to maximize protection of attorney-client privilege and work product protection.

- ***Engage Outside Counsel at the Outset of the Incident***

The court stressed timing of retention of counsel as a factor in preserving privilege. FirstEnergy brought in outside counsel “as soon as” the DOJ complaint was unsealed, and subpoenas were issued. (No. 24?3654, slip op. at 4–5 (internal citations omitted).)) Jones Day was retained to investigate the allegations and advise on the response to the criminal investigation; within a week, the board retained Squire to conduct its own investigation

and advise on potential exposure. That swift, parallel engagement signaled that both management and the board viewed the situation as a legal event requiring specialized legal guidance.

Serious cyber incidents often present similar legal risk from day one, particularly when personal data is implicated, critical operations are disrupted, or contractual notification obligations are in play. In that context, organizations should involve outside IR counsel at or near the outset, not at the end, of the investigation. Engagement terms should make clear that counsel is retained to advise on legal risk, regulatory obligations, and litigation exposure, and to direct the investigation in light of those risks. Board and executive communications should reflect that the incident is being treated as a legal, not merely operational, event.

- ***Counsel Must Meaningfully Direct the Investigation***

Timing alone is not enough. The court also focused on the substance of counsel's role. FirstEnergy and its board asked outside counsel for analysis and legal advice on how to respond to the significant legal risk they faced. Squire Patton Boggs met frequently with directors to discuss investigative findings, legal analyses, and assessments of potential criminal and civil liability. Jones Day conducted its own investigation and examined relevant records in connection with responding to the DOJ and "analyzing what acts occurred, whether those acts were illegal, and what criminal and civil consequences might ensue."

In other words, outside counsel did not simply receive copies of reports or rubber stamp business decisions; they ran the investigations, interpreted the facts and provided legal guidance.

In the IR context, a privileged, *FirstEnergy*-style investigation should involve counsel defining the scope of the forensic work and the questions to be answered, with the forensic firm engaged by or through counsel and its deliverables directed to counsel. Counsel should review forensic reports and underlying data and translate those findings into legal analysis—liability, regulatory obligations, notification decisions, and litigation strategy. Throughout the process, counsel should participate in briefings with the IR team and senior leadership, presenting investigative findings, explaining their legal implications, and advising on next steps.

If the technical team runs the investigation independently and counsel's involvement is limited to reviewing a completed technical report, a court may conclude the investigation was business led, not legally driven, weakening privilege and work product arguments across the incident lifecycle.

- ***Dual Legal and Business Purposes Do Not Defeat Privilege or Work Product Protection***

The district court concluded privilege did not apply because FirstEnergy used the investigations and associated legal advice to subsequently inform business decisions. The Sixth Circuit rejected that rationale as inconsistent with how companies function. The question is whether the company sought legal advice; the fact that it later used that advice for business purposes does not destroy privilege. Companies routinely consult attorneys about problems that arise in the course of business, and that fact alone does not strip communications of their fundamentally legal character.

On work product, the court reaffirmed the "because of litigation" standard: materials are protected if they are created because of or reasonably anticipated litigation, even if they also serve business objectives. In *FirstEnergy*,

the shareholder lawsuits and DOJ investigations supported the assertion that FirstEnergy's internal investigations were driven by actual and reasonably anticipated litigation.

In the IR context, investigative findings almost always serve dual purposes. Legally, findings are used to evaluate breach-notification obligations, defend potential claims, determine contractual requirements, and guide potential resolution options. Operationally, organizations use the same findings to fix affected systems, safely restore operations, improve security, and coordinate with potentially affected customers and vendors on their response.

FirstEnergy confirms that this dual use is not disqualifying. An IR investigation can remain privileged and be protected work product even if its findings are used to inform business decisions—for example, whether to shut systems down, what to tell customers, or how to address vendor relationships. What matters is that the investigation is undertaken because of legal and regulatory risk, and that counsel is engaged to provide legal advice on that risk.

Practically, engagement letters and statements of work should clearly state the legal purpose of the investigation, make explicit that outside counsel is directing and supervising the work, and provide that key written work product and communications are routed through counsel. This structure reinforces that legal advice and anticipated litigation are the driving forces behind the investigation, even though the same findings support business decisions.

- ***Sharing Information With 'Friendly' Third Parties Is Not Automatically a Waiver***

The Sixth Circuit's discussion of disclosures to FirstEnergy's auditor is particularly relevant to IR investigations, which often involve multiple third parties—auditors, cyber insurers, managed security service providers, forensic vendors, and customers or partners. The court held that sharing non privileged information with an auditor does not waive privilege; waiver occurs only as to privileged communications actually disclosed. It also emphasized that work product protection is not automatically waived by disclosure to a third party and is typically waived only by disclosure to an adversary or someone likely to become one. An independent auditor is not an adversary, particularly where ethical rules and professional obligations require confidentiality and withdrawal in the face of litigation against the client.

Applied to IR matters, *FirstEnergy* supports several practical distinctions. Organizations may be able to share factual summaries—timelines, high level descriptions, remediation status—with third parties without necessarily waiving privilege over counsel's underlying analysis or mental impressions. Work product protection is more likely preserved where the recipient is not an adversary, is contractually or ethically bound to maintain confidentiality (like the auditor in *FirstEnergy*), and is aligned with the company's interests. Care is required when dealing with third parties in the IR context, which can include customers, vendors, or other stakeholders who might become adverse; in those situations, limiting what is shared to factual descriptions and omitting counsel's legal analysis can help preserve privilege and work product protection even if relationships later deteriorate.

Outside counsel plays a central role in identifying which third parties can appropriately receive information, determining what can be shared as factual, non-privileged content, and ensuring that privileged communications and legal strategy remain within a tightly controlled circle.

PUTTING FIRSTENERGY INTO PRACTICE FOR INCIDENT RESPONSE

Taken together, *FirstEnergy* supports an IR model in which:

- Counsel is engaged early, as soon as a cyber incident is identified;
- Counsel initiates, directs and supervises the investigation, including the work of forensic vendors;
- The investigation is undertaken because of legal and regulatory risk, even though it may also serve subsequent business needs and inform related decision making; and
- Information is carefully shared only with limited and aligned third parties, focusing on factual content while preserving privileged legal analysis and work product.

While that framework may appear straightforward, the reality is that many security and IT teams operate in silos and are not always aware of the proper, legally informed protocols for privileged investigations. Legal involvement remains crucial to preserving privilege and protections—and that involvement must occur at the outset of an incident, not after key decisions have already been made.

Businesses should also be talking about these issues now, before an incident occurs, so they understand the right protocol to follow when an event does happen. An effective way to have these conversations is through tailored tabletop exercises that simulate realistic incidents, surface gaps in coordination or escalation, and create concrete, written plans to address those gaps. Those exercises help build a culture of cybersecurity across the organization by reinforcing that cyber risk is an enterprise-wide issue—not just a security or IT concern—and by transforming incident response from a last-minute scramble into a disciplined, defensible process that protects the business when it matters most, while maintaining the types of privileges that allow a full and candid assessment of the cyber incident and the path forward.

Sadia Mirza, *a partner with the Troutman Pepper Locke, leads the firm's incidents + investigations team, advising clients on all aspects of data security and privacy issues. She is the first point of contact when a security incident or data breach is suspected, and plays a central role in her clients' cybersecurity strategies.*

Tim St. George,*a partner with the firm, defends institutions nationwide facing class actions and individual lawsuits. He has particular experience litigating consumer class actions, including industry-leading expertise in cases arising under the Fair Credit Reporting Act and its state law counterparts, as well as litigation arising from data breaches.*

Kaitlin Clemens, *an associate based in the firm's Philadelphia office, handles ransomware and data extortion cases, and advises on compliance with state and federal laws, including HIPAA, FERPA, and GLBA, as well as development of privacy programs and pre-incident response strategies, as well as creating and delivering comprehensive training for attorneys who are new to cybersecurity.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber