Articles + Publications | March 12, 2026

# How ‘FirstEnergy’ Could Shape Privilege Battles in Post-Breach Litigation, Part 3

**WRITTEN BY**

Sadia Mirza | Timothy J. St. George | Kaitlin J. Clemens | Jennifer L. Brumfield

*This article was originally published on* The Legal Intelligencer *and is republished here with permission as it originally appeared on March 12, 2026.*

In this third and final article in a three-part series on the *FirstEnergy* decision, we turn to what happens when litigation arrives and privilege is challenged.

Over the past several years, district courts have been skeptical of privilege claims over forensic investigation materials in the cybersecurity context. *FirstEnergy* provides a framework for defending those materials. Every cyber investigation serves two purposes. From a legal perspective, the investigation informs litigation exposure and defense strategy. But the same investigation also identifies compromised systems, drives remediation and supports business operations. After *FirstEnergy*, those dual purposes do not defeat privilege, provided the investigation was initiated because of legal risk and directed by counsel. This article also examines how the lessons of *FirstEnergy* apply in cases involving multiple defendants that may have both a desire and need—for both business and legal purposes—to work together to understand an incident and share information.

## Anticipating How Plaintiffs Will Challenge Privilege After ‘FirstEnergy’

Before the *FirstEnergy* decision, federal district courts often ordered production of forensic reports that defense counsel argued were protected by privilege. See, e.g., *In re Premera Blue Cross Customer Data Security Breach Litigation*, 296 F. Supp. 3d 1230 (D. Or. 2017); *Wengui v. Clark Hill,* 2021 WL 106417 (D.D.C. Jan. 12, 2021).

One exception is *In re Target Customer Data Security Breach Litigation*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015), where the court upheld privilege over materials produced through a genuine “two-track” investigation, one for the business response and a separate track directed by counsel to inform legal advice and prepare for litigation.

Despite *FirstEnergy*’s protective reasoning and affirmance of privilege, plaintiffs will continue to challenge privilege in post-breach litigation, including by reference to contrary authority. Preparing a defense starts with anticipating how plaintiffs will challenge privilege and constructing a protective regime from the very beginning of an incident.

### ‘The Investigation Was Business-Led, Not Legal Tactic’

Pre-*FirstEnergy*, courts first focused on investigations that serve both legal and business purposes. The decisions

principally analyzed whether a forensic report would have been created in substantially similar form, regardless of litigation. *FirstEnergy* addresses this concern by highlighting when and why investigations were commissioned. The court concluded that materials are protected "even if they also serve business or compliance purposes, so long as they would not have been generated in substantially similar form in the absence of the threat of litigation."

Plaintiffs will attempt to distinguish *FirstEnergy* on the ground that cyber incidents typically begin as business events. Security teams often detect security incidents. IT triages them, and management is generally notified before counsel is called. Plaintiffs will argue the response was business-led, not legal. The strength of the privilege argument credited by *FirstEnergy* will depend on the factual record. If the organization delayed engaging counsel, or if early forensic work was initiated and directed solely by IT or security teams, then the anti-privilege argument gains traction. Organizations that treat the incident as a legal event from the start, engage counsel immediately, and document counsel's direction of the investigation will be best positioned to rely on *FirstEnergy*'s legal framework.

**'The Role of Counsel Was Nominal, Not Substantive'**

Even when papered appropriately, plaintiffs will argue that counsel's name may have been on the engagement letter, but in practice the forensic vendor reported to the security team that set the scope of work, and that counsel merely received copies of reports. If counsel's involvement was cosmetic rather than substantive, then the investigation may not qualify for protection under *FirstEnergy*.

To assess privilege, courts will analyze the contemporaneous record: engagement letters, statements of work, emails, meeting notes, and counsel declarations. Evidence that counsel played a passive or after-the-fact role will weaken the privilege claim. To invoke the *FirstEnergy* holding, counsel should take active roles in defining the forensic scope, reviewing and shaping deliverables, participating in investigative briefings, and translating forensic findings into legal analysis.

**'The Forensic Report Is a Business Record, Not Work Product'**

Plaintiffs will argue that the forensic report was created to understand and fix any security issues and restore operations—not because of anticipated litigation—and that a substantially similar report would have been created regardless of any legal proceeding, thereby defeating the claimed privilege.

*FirstEnergy*'s reasoning provides a strong counter to the line of precedent holding that forensic reports are business-related documents and not privileged. But the privilege argument is strongest when the organization can show a clear split between the counsel-led investigation and the subsequent operational response. A FirstEnergy approach recognizes that investigations ensuring business continuity operate differently than investigations triggered by litigation threats. The differentiating factor is whether the probe would have taken this form without the prospect of litigation.

**'Privilege Was Waived by Disclosure'**

The widespread distribution of forensic findings has proven fatal in several district court cases. In *Clark Hill,* sharing the report with IT personnel and the FBI was cited as evidence that it served nonlitigation purposes.

But *FirstEnergy* takes a more nuanced view of third-party disclosures, holding that sharing factual findings with nonadverse third parties does not automatically waive privilege over the underlying communications or counsel's mental impressions. And the court emphasized that sharing bare factual conclusions is of a different nature than revealing the mental impressions and thought process behind counsel's litigation strategy.

Plaintiffs will still contend that even if privilege existed, it was waived by the organization's post-incident disclosures. Common targets include disclosures to regulators, insurers, and auditors, or public statements and SEC filings. Plaintiffs may also point to broad internal distribution of forensic findings as evidence that the materials were not treated as privileged.

*FirstEnergy*'s framework is helpful here. The court distinguished factual conclusions from privileged legal analysis, holding that releasing "ultimate findings" does not waive the privilege protecting the underlying analysis. The court also reaffirmed that work product protection is generally waived only by disclosure to an adversary, and that disclosures to auditors and regulators do not automatically trigger waiver.

*FirstEnergy* does not eliminate the risk that sharing the details of forensic reports with broad audiences will waive privilege, particularly if the disclosed materials contain counsel's mental impressions or legal analysis. Post-*FirstEnergy*, litigators must show that disclosures contained only facts, went to non adverse parties bound by confidentiality, and excluded privileged analysis.

## Protecting Privilege Across Multiple Parties

Unlike the situation in *FirstEnergy* where the defendant sought privilege of its own internal investigation, cybersecurity incidents increasingly implicate multiple parties, including when the customers of a breached entity are also named as defendants. Co-defendants may form a joint defense group to pool resources and coordinate litigation strategy. The *FirstEnergy* conceptual framework also is helpful for protecting privilege in these multi-party scenarios.

### Protecting Privilege in Joint Defense Groups

The common interest doctrine permits parties that share a common legal interest to exchange privileged materials, disclose litigation strategy, and share experts and reports under a joint defense agreement (JDA) without waiving the underlying privilege. *FirstEnergy*'s treatment of third-party disclosures support the use of a JDA to share otherwise privileged materials. Under *FirstEnergy,* a shared forensic expert retained by counsel for a joint defense group would qualify for work-product protection, provided the engagement is structured to inform litigation strategy. And because disclosures among co-defendants who share a common legal interest are, by definition, nonadversarial, there would be no privilege waiver under the *FirstEnergy* framework.

That said, the common interest doctrine requires that an underlying privilege exist before any sharing occurs, that the parties share a common legal interest and not merely a commercial one, and that the exchange of information is made in furtherance of that shared legal interest. *FirstEnergy*'s emphasis on the contemporaneous record applies with equal force to multi-party arrangements. A written agreement articulating the shared legal interest and the group's commitment to confidentiality should be in place before materials are exchanged. Counsel, not the business, should retain any shared experts, and the experts' scope of work should make clear that the purpose is

to inform legal strategy, not just to share in costs. Communications with the expert should be routed through counsel and documented. Reports and documents circulated within the group should be clearly marked as privileged and confidential, and restricted from further distribution where possible. Because the potential exists for members of the group to become adversarial to one another at a later date—for example, if crossclaims get filed or an indemnification dispute arises—the JDA should also address a departing member's obligation to keep privileged documents confidential.

**Sharing Incident Response Reports With Customers**

Another multi-party example occurs when the vendor that suffers a breach discloses information it learned from the forensic experts to its affected customers seeking that information. If the vendor and its customers are defending against claims by the same class of plaintiffs, materials exchanged in furtherance of that shared legal interest should remain protected under the common interest doctrine.

But vendor-customer relationships can be trickier than joint defense groups. The customer may blame the vendor for the breach, for instance. Courts have held that parties negotiating or potentially in dispute with each other cannot claim a common legal interest. In one recent example, a district court found that production of a shorter forensic analysis to "third-parties that themselves were potential litigants and adversaries" constituted a waiver of work product protection over the full forensic report, because the shorter document "revealed the goals, scope, methodology, and findings" of the broader investigation. See *In re American Medical Collection Agenc, Customer Data Securities Breach Litigation,* MDL No. 19-MD-2904, 2023 WL 8595741, at *12 (D.N.J. Oct. 16, 2023). Thus, potential indemnification claims and adversity should be considered before materials are shared.

*FirstEnergy'*s distinction between factual conclusions and privileged analysis provides a workable framework here too. Vendors can share factual findings about what happened, when, and what data was affected, but should withhold the litigation risk assessments or strategies. The shared information should be in a separate, non-privileged summary prepared specifically for customer distribution. A summary that discloses mental impressions related to the potential legal fallout of the incident, however, may be treated as a waiver of the privilege for the underlying report, even if the summary itself is shorter and less detailed.

**Conclusion**

*FirstEnergy* is a significant development for organizations seeking to protect post-breach investigations. It strengthens the privilege framework even when materials flow between multiple parties, but whether the privilege holds depends on the same factors as the single party context. Counsel must lead, the investigation must be structured for litigation, the evidentiary record must be built contemporaneously, and the sharing of privileged materials must be controlled, documented, and confined to parties with a genuine common legal interest.

*FirstEnergy*'s protections depend on active, written, and tested policies (through regular tabletop exercises) being implemented in real time. Organizations that use the structure described across this three-part series—engaging counsel early, directing investigations through counsel, structuring vendor relationships to support privilege, and building the evidentiary record in real time—will be best positioned to defend their privilege claims when those claims are challenged in post-breach litigation. And, those same considerations will extend to multi-party actions where co-defendants will often have both a business and legal need to share information and work together.

**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.*

**Jennifer Brumfield**, *an associate with the firm, represents clients in complex cybersecurity and privacy class actions that involve emerging legal questions related to statutory interpretation, jurisdiction, and standing. She manages all phases of litigation from case assessment through discovery, dispositive motions, settlement and appeals.*



**RELATED INDUSTRIES + PRACTICES**

- Privacy + Cyber