PUBLICATION

Cybersecurity Awareness Month 2025: How to Preserve Privilege in Cyber Investigations

Authors: Matthew George White, Alexander Frank Koskey, III, Madison J. McMahan
October 29, 2025

In the aftermath of a cyberattack, forensic investigations are often launched under intense pressure to identify what went wrong, why, and how to fix it. A common practice following such an investigation is the preparation of a forensic report detailing the results of the investigation. These reports can be invaluable in shaping a company's response and remediation efforts – but they can also become a prime target of discovery in litigation.

Recent years have seen a steady stream of court decisions narrowing the privilege protections for forensic reports, often with judicial scrutiny over whether these investigations truly served a legal purpose. While in the context of an internal investigation, rather than a data breach, the Sixth Circuit's recent decision in *In re FirstEnergy Corp. Securities Litigation* (Aug. 7, 2025) cuts the other way, reinforcing that privilege can still apply when companies take the right precautions and clearly establish that their investigations are directed toward obtaining legal advice.

These cases demonstrate the unsettled legal landscape: some courts are taking a restrictive view of privilege in cyber and internal investigations, while others – like the Sixth Circuit – recognize the practical reality that such investigations nearly always have both legal and business implications. The key is how they are structured, documented, and controlled from the outset. This alert provides practical guidance to best position your business to preserve privilege in a cybersecurity investigation.

Cases Narrowing the Privilege

As highlighted in our original "Privilege Under Fire" alert, decisions such as *McClure v. Medibank Private Limited* [2025] FCA 167, *In re Capital One Consumer Data Security Breach Litigation* (E.D. Va. 2020), and *Guo Wengui v. Clark Hill, PLC* (D.D.C. 2021) have emphasized how easily privilege can be lost when forensic reports are used (or even described publicly) as serving operational or business purposes.

In *McClure*, the Federal Court of Australia ordered production of three Deloitte forensic reports prepared in response to a data breach, finding that the reports were primarily intended for governance, regulatory, and transparency purposes rather than legal advice. Likewise, U.S. courts in *Capital One* and *Clark Hill* found that even reports commissioned through counsel were not privileged where they served overlapping operational roles, were paid for by IT departments, or were widely shared internally or with regulators.

These cases collectively underscore that privilege claims fail when legal purpose is not dominant, well-documented, and preserved through careful handling and limited disclosure.

The *FirstEnergy* Decision

In light of these trends, the Sixth Circuit's *FirstEnergy* decision provides a balancing perspective and renewed confidence for organizations facing challenging internal or cyber investigations.

The case arose from an internal investigation launched after the indictment of former Ohio House Speaker Larry Householder on bribery charges implicating FirstEnergy. Following the investigation, shareholders in a

securities class action sought production of the investigative materials, arguing that the attorney-client privilege did not apply because the company used the findings for both legal and business purposes.

The district court agreed and ordered production. On appeal, the Sixth Circuit stayed that order, concluding that the lower court's approach was too narrow. The appellate court emphasized that what matters for attorney-client privilege is whether the company sought legal advice – not how it later used that advice. Because FirstEnergy's counsel had conducted the investigation in response to subpoenas, lawsuits, and potential enforcement actions, the court found that the materials were likely protected by both the attorney-client privilege and the work product doctrine.

This decision reaffirms that the mere existence of a business component does not destroy privilege. In today's world, internal and cyber investigations inevitably have mixed purposes. If a company can clearly demonstrate that its primary purpose for conducting an investigation was to obtain legal advice – and this intent is thoroughly documented – courts are more likely to uphold privilege protections, even when business considerations are also present.

Contrasting Judicial Approaches

FirstEnergy stands in contrast to cases like *Capital One* and *Clark Hill*, showing that courts are not aligned on how to evaluate privilege in the context of investigations following cybersecurity or compliance events.

Taken together, these rulings reveal a clear split in judicial perspectives:

- Restrictive approach (e.g., *McClure*, *Capital One*, *Clark Hill*): Privilege fails where reports appear primarily intended for operational or regulatory purposes, regardless of counsel's involvement.
- Protective approach (*FirstEnergy*): Privilege may be upheld when a company can demonstrate that its primary purpose for conducting an investigation was to obtain legal advice, and this intent is thoroughly documented – even if the findings are subsequently used for business or governance purposes.

This inconsistency underscores the critical takeaway: companies cannot rely on privilege labels, subject lines, or assumptions. Courts will probe the underlying purpose, process, and structure of the engagement to determine whether the privilege truly applies.

Practical Guidance: Structuring Investigations to Preserve Privilege

Whether courts lean restrictive or protective, they consistently look for the same foundational safeguards. Companies that take the following steps at the outset are far better positioned to sustain privilege claims:

- **Engage forensic vendors through counsel:** Outside counsel should retain and direct the engagement. The purpose should be explicitly tied to providing legal advice and preparing for potential litigation.
- **Document the legal purpose:** Include language in engagement letters, memos, and communications that the investigation is being conducted to support legal advice, not merely operational recovery.
- **Separate legal and business workstreams:** Consider distinct vendors, teams, or scopes of work for remediation and legal analysis.

- **Restrict distribution:** Limit access to privileged reports to those assisting counsel. Prepare a separate, non-privileged summary for regulators, boards, or the public if needed.

- **Be mindful of waiver risks:** Avoid citing or referencing privileged findings in public statements or regulatory submissions.

- **Engage experienced counsel early:** Privilege cannot be applied retroactively. Bringing in experienced outside counsel at the start of an incident ensures their ability to properly structure the engagement, create appropriate documentation, and maximize privilege claims.

Ultimately, the Sixth Circuit's *FirstEnergy* decision shows that privilege may not be lost simply because investigations have dual purposes. When companies can demonstrate that they sought legal advice through counsel and took care to maintain confidentiality, courts may uphold privilege – even amid overlapping business imperatives. However, until courts cease diverging on how they evaluate mixed-purpose investigations, or until the Supreme Court of the United States weighs in, there will be a risk of compelled disclosure of forensic reports. The best protection lies in deliberate, early-stage planning to ensure privilege is clearly established and defensible from day one.

If you need guidance on establishing procedures to protect privilege, responding to a cybersecurity incident, conducting tabletop exercises, or defending against data breach litigation, don't hesitate to contact the authors, Matt White, Alex Koskey, or MJ McMahan, or any other member of Baker Donelson's Incident Response Team. We regularly assist clients in navigating these high-risk moments with clarity, efficiency, and strategic focus. Our team also advises on a broad range of cybersecurity, data privacy, and technology matters – whether proactive or reactive. We're here to help.

October is National Cybersecurity Awareness Month

Observed annually in October, Cybersecurity Awareness Month is a collaborative effort between the public and private sectors to raise awareness about cybersecurity. It was launched in 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA).

Throughout Cybersecurity Awareness Month, we will provide proactive tips and information in order to mitigate your cyber risks.