

When Research Goes Wrong:

Responding to Research Misconduct

Safeguarding Institutional Integrity: Definitions,
Case Studies, Enforcement & Prevention



Melissa Markey
Attorney
mmarkey@hallrender.com



Rebecca Merrill
Attorney
rmerrill@hallrender.com

Hall Render content is intended for informational purposes only. For ethical reasons, Hall Render attorneys cannot—outside of an attorney-client relationship—answer specific questions that would be legal advice.



CLE Information

Disclaimer: Course Codes for Attendance Verification

To verify your attendance for this course, please note the following:

- **Live Sessions:** There are **two unique course codes** that you need to note. These codes will appear on various slides throughout the presentation.
- **On-Demand Sessions:** Similarly, there are **two separate codes** for on-demand sessions. These codes can also be found on multiple slides within the presentation.

Please make sure to record these codes accurately, and at the end of the session, simply scan the QR code to enter the course codes and confirm your attendance.

At the end of the session, simply scan the QR code to enter the course codes and confirm your attendance.



Live Course Code #1:
SAMPLE



On-Demand Course
Code #1: **SAMPLE**

Speakers



Melissa L. Markey
Shareholder
Hall Render



Rebecca Merrill
Shareholder
Hall Render



Speakers Note

On behalf
of our
speakers,
we note:

The views and opinions expressed in this presentation are solely those of the authors and presenters and do not necessarily represent the views of Hall Render or any other organization.

This presentation is for educational and informational purposes only and does not constitute individualized legal advice. Further, this presentation does not establish any form of attorney-client relationship. Organizations facing an ORI inquiry or FCA investigation should consult qualified legal counsel.

The authors and presenters, their organizations, and the professionals thereof, entities related thereto and professionals thereof, and clients of those organizations and entities related thereto, are not bound by this presentation; nor are they responsible for any errors or omissions in this presentation.

Agenda

1. What counts as research misconduct
2. The grey zone: questionable research practices
3. How big is the problem and what does enforcement cost?
4. Case studies
5. Why institutions catch it late
6. Detection tools and signals
7. Prevention: culture and controls
8. The investigation process: institutional, ORI, and DOJ
9. A 12-month roadmap
10. Board & C-suite talking points
11. Be aware of parallel proceedings



1. What counts as “Research Misconduct”?

Narrow Definition, Wide Exposure

Fewer than a dozen federal misconduct findings are made each year. False Claims Act settlements in this space run from \$5M to \$112M. The gap between those two numbers is where the real exposure sits.

Research Misconduct Defined

Part 93 Definition

We start with the types of misconduct:

- **Fabrication**: making up data or results and recording or reporting them
- **Falsification**: manipulating materials or processes or changing or omitting data so the record is not accurately represented
- **Plagiarism**: appropriating another person's ideas, processes, results, or words without credit
- **What is the legal test?** (42 C.F.R. §§ 93.103–93.106)
- **Who enforces it?**

2. The Grey Zone

The Grey Zone: *Other Types of Questionable Research Practices (QRPs)*

- Far more common than FFP
 - P-hacking and selective outcome reporting
 - HARKing
 - Dropping inconvenient conditions or subjects
 - Gift, ghost, and coerced authorship
 - Undisclosed conflicts
 - Salami-slicing
- Why leadership should care:
 - QRPs are rarely sanctionable but corrode the literature at scale
 - Self-report studies find roughly 2% of researchers admit fabricating or falsifying, while around a third admit questionable practices
 - Today's tolerated shortcut is tomorrow's investigation
 - Policy addressing only FFP leaves most of the risk ungoverned

Practice Point:
QRPs are rarely sanctionable under Part 93,
but the federal grant certifications built on them can create FCA exposure

Legal Test & Enforcement Tracks

- **The three-part test (42 C.F.R. §§ 93.103–93.106)**
 1. A significant departure from accepted practices of the relevant research community
 2. Conduct committed intentionally, knowingly, or recklessly
 3. Proof by a preponderance of the evidence
- **What is excluded?**
- **What is the scope?**
- **The three enforcement tracks**
 1. Institutional inquiry
 2. ORI oversight
 3. DOJ civil, False Claims Act

CLE Course Code #1

*At the end of the session, simply scan the QR code for **live** or **on-demand** session to enter the course codes.*

CLE Course Code #1

Live Course Code #1: **Research-Live**



Attending on **October 6:**
Use Live Course Code

Please make sure to **record these codes accurately**, and at the end of the session, simply scan the QR code to enter the course codes and confirm your attendance.

ON-DEMAND COURSE CODE

On-Demand Course Code #1:
OD-Research

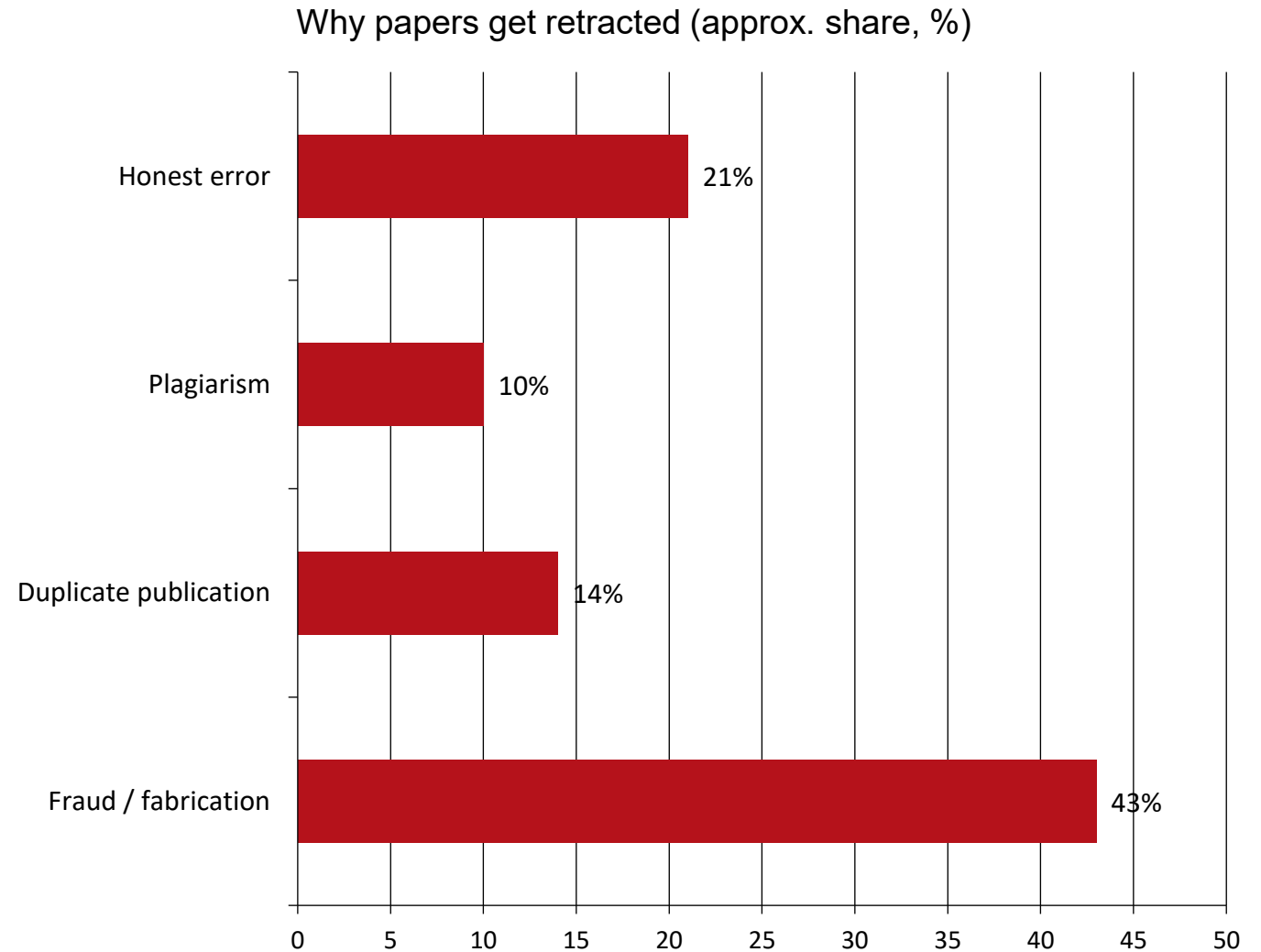


Attending on **On-Demand** (*after 10/6/26*):
Use On-Demand Course Code

3. How Big is the Problem?

How Big Is the Problem?

- Retractions have risen faster than publication volume, passing 10,000 in a single year for the first time in 2023 – why?
- Analyses of the retraction record attribute roughly $\frac{2}{3}$ of retractions to misconduct
- This is the scientific scale
- Enforcement is expected to follow



Enforcement Numbers

Scale of the regulated system

1. ORI research misconduct findings: ~10 to 15 per year
2. NIH-funded institutions: 2,500+
3. Annual PHS research funding: \$50B+
4. Typical FCA research-fraud settlement amounts: wide range
5. FCA recoveries (All Healthcare) — ~\$1.67B (2024) to ~\$5.7B (2025)

The Enforcement Evolution

- The evolution of allegations
 - Historically, allegations relied on internal whistleblowers witnessing dry-labbing or overt data fabrication
 - Today, allegations are increasingly driven by external data sleuths using industrial-scale image analysis and statistical forensics
- Technology
 - Integration of AI-driven tools (e.g., Proofig and ImageTwin) enable regulators, journals, and whistleblowers to scan thousands of published Western blots, micrographs, and data arrays simultaneously
- Faster ORI response; increased DOJ coordination
- The Iceberg Effect: Unresolved Exposure vs. ORI Findings
- The Core Question: It's not a question of whether, assume it is a question of when
- Discussion Question: If detection is now automated and external, how should we proactively audit our own published data before someone else does?

Discussion Question

If detection is now automated and external,
should institutions proactively audit their own published data before someone else does?

4. Case Studies

Three Cases, Three Failure Modes

Each was exposed by outsiders, not by the institution that employed the researcher.

Andrew Wakefield



- UK physician who published a notorious 12-patient study in The Lancet claiming a causal link between the MMR vaccine and autism in 1998.
- Investigative journalism uncovered that Wakefield had undisclosed financial ties to lawyers pursuing litigation against vaccine manufacturers and found that all 12 cases contained misrepresentations or undisclosed alterations that could not be reconciled with the underlying medical records.
- Failure mode: peer-review blindness to material conflicts of interest, over-reliance on a small uncontrolled case series of 12 patients, and inadequate pre-publication data validation.
- The control that would have caught it:
 - Mandatory open-access trial registries
 - Prospective registration of research protocols + prespecified methods/outcomes
 - Universal financial disclosure tracking
 - Independent source-data verification or full or sample audit of records prior to journal acceptance
- Fraud latency impacts public health decades later. Data integrity is a matter of patient-safety and public-health control, not just academic ethics.
 - The paper was published in 1998 and not fully retracted until 2010; its effects on vaccine confidence continued long after the scientific claims had been discredited.

Wakefield Discussion Points

- How would peer-review or IRB process catch a 12-patient study with undisclosed litigation funding?
- Who at your institution verifies raw clinical data before publication — and would they have access?
- What would we do if a high-profile finding of ours were challenged publicly years after publication?
- Are your institution's conflict-of-interest disclosures verified or self-reported and filed away?
- If an allegation surfaced tomorrow, how fast could your institution sequester the underlying data?

Jan Hendrik Schön

- Bell Labs physicist who published breakthrough molecular-electronics results at an extraordinary rate around 2000–2001.
- A 2002 investigation found at least 16 counts of misconduct: data substituted and identical curves reused across unrelated papers.
- Failure mode — no raw data retained, failed independent replication, and a star-producer culture that suppressed doubt.
- The controls that would have caught it:
 1. Mandatory raw-data retention with a documented chain of custody
 2. Independent validation / replication before publication
 3. Escalation of outliers – e.g., publication volume
- Output velocity is a risk indicator, not only a success metric.



Schön Discussion Points

- Would your institution notice a researcher publishing at an impossible rate — or celebrate it?
- Who retains the raw data behind your published figures, and for how long?
- Is there any independent replication or review of results before they leave your institution?
- Would a junior colleague who doubted a star producer's data have somewhere safe to raise it?
- Could you detect the same figure reused across two unrelated papers from your own labs?

Paolo Macchiarini



- Three synthetic trachea transplants at Karolinska University Hospital under Macchiarini's leadership (2011 – 2013).
- Published outcomes did not match patient records, and two of the three patients died.
- Four whistleblowing physicians were disciplined
- External journalism, not internal process, forced the reckoning.
- The vice-chancellor and closes colleagues resigned.
- Failure mode: 1. reputational defense of a celebrity recruit +
 2. retaliation against internal reporters

The control that likely would have caught it:

- Enforced non-retaliation protection and a reporting channel that bypasses the recruiting chain.

Macchiarini Discussion Points

- If a clinician raised concerns about a celebrity recruit here, who would hear it? Who would they report to?
- Can a reporting channel at your institution bypass the chain that did the recruiting?
- How would you know if published outcomes did not match the patient records?
- What protects a whistleblower here from being investigated instead of the allegation?
- At what point does a research-integrity problem become a patient-safety problem? Who makes that call?

The Image-Integrity Era

Moving From Closed Committees to Public Digital Auditing & Oversight

What changed

- Forensic sleuths and PubPeer screen figures in public
- Spliced panels stay detectable years later
- 2022–2024 reviews reached a university president

What it means for you

- Allegations arrive public, evidenced, and first
- Hour one is sequestration, comms, and privilege
- Screening costs less than post-publication defense

The Enforcement Overlay

The Modern Data Risk Paradigm

The 2025 settlement

- \$15M settlement over NIH-funded research
- 14 publications, six grants, images altered
- Surfaced by an external data sleuth — who took \$2.6M

What it establishes

- Public image allegations are a qui tam pipeline
- The relator sat outside the institution
- No misconduct finding was required

5. Why Institutions Catch Misconduct Late

Why Institutions Catch It Late

- Incentives reward volume and novelty
- Conflicted gatekeeping
- Weak data custody
- Whistleblower risk
- Process opacity
- No muscle memory

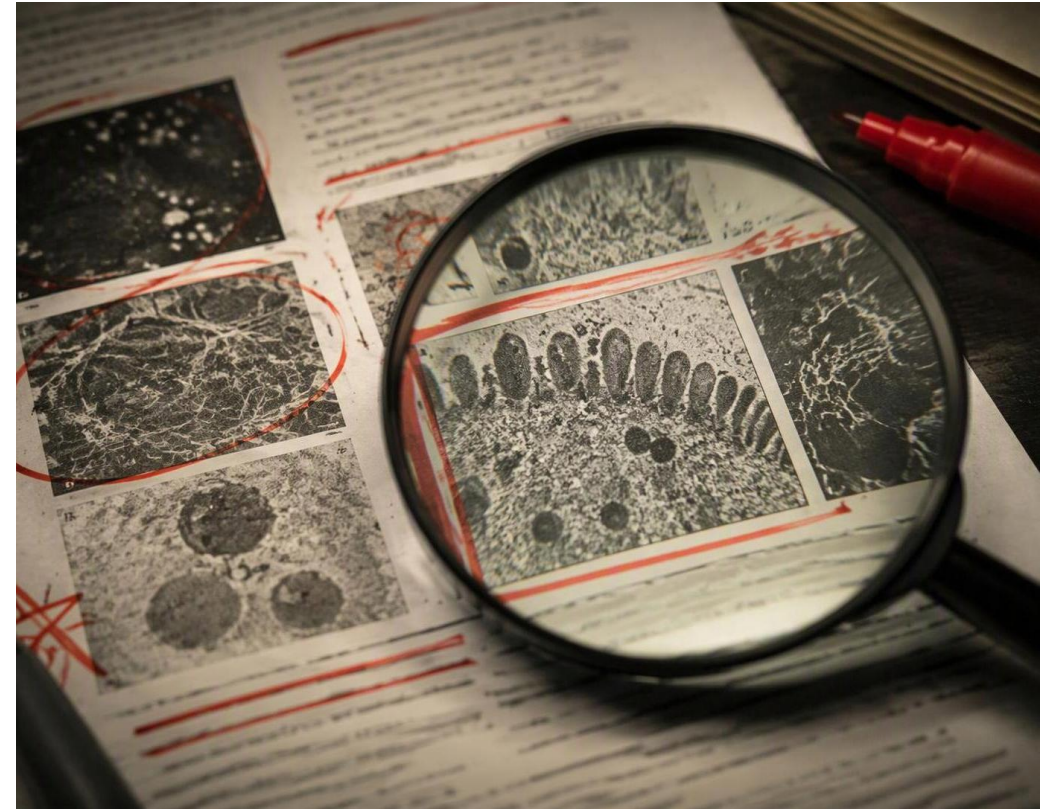
6. Detection Tools & Signals

*Controls that are cheap before publication &
ruinous to retrofit afterwards*

Detection Toolkit: *Shifting from Passive Ethics Frameworks to System-Level Infrastructure Controls*

The Paradigm: Screen before you publish,
not after you are accused.

1. Automated Integrity Screening
2. Centralized Data Custody
3. Forensics & Analytics
4. Continuous Auditing
5. Isolated Reporting Pipeline
6. Public Record Surveillance



Early Warning Signs and Monitoring

Red flags

- **Data** — too perfect, impossible timelines
- **Misleading Statistics** — unusual frequencies or distributions
- **Supply Chain** — misalignment throughput v logs
- **Publications** — reused images, retractions
- **Gift or Ghost Authorship**
- **Salami Slicing**
- **Lab culture** — turnover, PI complaints, isolation
- **Behavioral** — tight control of the raw files
- **Metadata Deletion** — Unexplained loss of raw data
- **Pre-Print Divergence** — Unexplained alterations
- **External** — PubPeer comments and anonymous tips

What to monitor

- Routine audits of high-risk research
- Data-integrity spot checks
- Exit interviews for departing lab members
- PubPeer monitoring of your affiliations
- ELN Compliance and System Metadata Logs
- Supply Chain & Procurement Reconciliation
- Author Velocity & Co-Authorship Anomaly Vectors



No single signal is proof —
clusters are the trigger.

CLE Course Code #2

*At the end of the session, simply scan the QR code for **live** or **on-demand** session to enter the course codes.*

CLE Course Code #2

Live Course Code #1: **Misconduct-Live**



Attending on **October 6:**
Use Live Course Code

Please make sure to **record these codes accurately**, and at the end of the session, simply scan the QR code to enter the course codes and confirm your attendance.

ON-DEMAND COURSE CODE

On-Demand Course Code #2:
OD-Misconduct



Attending on **On-Demand** (*after 10/6/26*):
Use On-Demand Course Code

7. Prevention Culture & Controls

Prevention: Culture and Control

Culture

- Independent oversight
- Systemic Competence
- Accountability at the top
- Enforced non-retaliation protection for reporters
- Value structure realignment

Controls

- Institutional data custody, seven-year retention
- Lab notebooks with immutable audit trails
- Pre-publication data screening
- Authorship agreed in writing at project start
- Pre-registration; annual conflict disclosure

Emerging Risk: AI in Research

Where the risk sits

Federal Guidance Baseline

- Formal ORI AI Guidance maps generative AI to 42 CFR Part 93
- Disclosure is required but does not serve as a safe harbor if the tool usage violates accepted research practices

AI-Generated Content & Hallucinated Citations

- Text: Undisclosed use in grants/manuscripts
- Citations: Hallucinated references constitute FFP if they manipulate literature reviews or distort foundational baselines

AI Image & Structural Fabrication

- Utilizing generative AI to synthesize, stitch, or artificially alter data constitutes overt fabrication

AI-Assisted Analysis & Data Falsification

- Running opaque LLM scripts that obscure analytical outliers or applying generative "smoothing/enhancement" to raw files constitutes falsification

Act now

Adopt Formal AI Governance

- Institutional research-specific Generative AI Policy
- Clear operational boundaries for data generation versus administrative drafting

Mandate Comprehensive Tool Disclosure

- Require explicit disclosure of AI tools used, data ingested, and prompt workflows used in papers and grants

Prohibit Standalone "Detector" Reliance

Enforce Pipeline Archiving & Verification

- AI-assisted analytical pipelines, custom prompts, and code arrays to be archived in the ELN for verification and reproducibility

The Part 93 Sequence

- 1. Assessment:** Immediate. Does the allegation meet the definition, and is PHS funding implicated?
- 2. Inquiry, 60 days:** Measured from opening the inquiry; the 2024 Rule changed the trigger from allegation received. Good-faith notice to the respondent at or before the start; the respondent may comment on the inquiry report.
- 3. Investigation, 120 days:** Written notice to ORI on or before the date it begins. The respondent gets 30 days to comment on the draft report.
- 4. Institutional decision:** Final determination; the complete record is forwarded to ORI.
- 5. ORI oversight review:** Close the matter, make findings and propose administrative actions, or elevate.
- 6. Appeal:** Respondent may contest before an ALJ at the HHS Departmental Appeals Board.



8. Investigation Process

The First 48 Hours: *Immediate First Steps*

- **Hours 0 – 4: *Immediate Sequestration and Privilege***
 - Notify GC/CLO
 - Engage outside counsel
 - Immediate digital sequestration; initiate physical sequestration
 - Identify custodians
- **Hours 4 – 24: *Chain of Custody & Containment***
 - Issue a litigation hold
 - Secure notebooks and samples
 - Establish timestamped inventory log of all sequestered assets
 - Identify key witnesses; schedule interviews
- **Hours 24 – 48: *Jurisdiction & Assessment***
 - Confirm PHS jurisdiction
 - Identify all potentially affected grants
 - Set the inquiry timeline
 - Conflict-screen committee members

The First 48 Hours: *Sequestration Protocol*

Compliance Checklist to Mitigate Institutional Obstruction Risk

Step 1: Immediate Digital Sequestration

- Network freeze
- Snapshot laboratory desktops, local hard drives, and cloud storage folders
- Hidden metadata preservation

Step 2: Physical Evidence Recovery

- Control access (e.g., physical locks, keycard access, equipment, storage, vendors, partners)
- Gather devices (e.g., laptops, tablets, external hard drives, portable storage media)
- Paper and sample collection and sequestration

Step 3: Chain-of-Custody Documentation

- Tamper-evident logging of sequestered physical items
- Centralized master inventory log (e.g., where, when, and method of seizure; custodian; chain of custody)
- Secure storage

Step 4: External Escalation Check

- Consider engaging (through legal counsel) third-party forensic experts for complex cases

Practice Note:
Failure to properly
and timely sequester
can support an
obstruction finding
against an institution

Respondent Rights & Committee Composition

Respondent rights

- Skip one and ORI can reject your findings
- Written notice of the allegation
- Access to the evidence before interview
- Opportunity to respond before findings are made
- Counsel or an advisor present at any interview
- Comment on the draft investigation report

Who cannot serve?

- Prior collaborators
- Direct competitors
- Active personal and/or professional disputes with respondent
- Co-author or mentor ties to respondent
- Financial or commercial entanglements
- Administrative superiors
- Insufficient scientific depth to evaluate the work

Practice Note

1. Provide meticulous notice
2. Build an unchallengeable record

9. 12-Month Roadmap

A 12-Month Roadmap

Immediate Compliance Validation (Days 0 – 90)

- Audit Historical Commitments
- Execute Structural Reporting Lines
- Codify the Recklessness Standard

Infrastructure Deployment & Sequestration Drills (Days 90 – 180)

- Build the Data Vault
- Stress-Test Sequestration
- Audit NIH DMS Compliance

A 12-Month Roadmap

Automated Screening & Public Monitoring (Days 180 – 270)

- Launch Pre-Submission Gates
- Deploy Continuous Surveillance
- Deliver PI-Specific Training

Incentive Realignment & Board Reporting (Days 270 – 365)

- Overhaul Promotion Criteria
- Execute Random Spot Audits
- Boardroom Accountability

The Paradigm for Success

Success looks like shorter detection latency and more reports, not fewer.

Post-Finding CAPA: *Remediate, Sustain & Communicate*

Remediate

- **Compliance program** — award conditions, controls plan
- **Research record** — retractions and journal notice
- **Personnel actions** — supervise, reassign, or separate

What to sustain

- **Enhanced oversight** — training, annual ORI reports
- **Reputation** — restore the cleared, shield reporters
- **Culture** — a commitment, not a concession

10. Board & C-Suite Talking Points

Board and C-Suite Talking Points

- **Financial exposure** — A single misconduct case can generate \$5–50M+ in False Claims Act liability, which can be exacerbated by follow-on donor clawbacks as well as reputational harm.
- **Talent** — Reputational damage drives faculty departures long after the case closes.
- **Insurance, not overhead** — Compliance infrastructure is protection against catastrophic loss.
- **The cost of silence** — Institutions that suppress concerns pay more later, not less.
- **Fiduciary Duty** — Corporate officers owe a strict, independent duty of oversight within their respective spheres.
- **Liability Standard** — If an executive (e.g., VP of Research) receives a material red flag and fails to engage in prompt review and risk mitigation (e.g., pause the draw down from impacted grants), the executive (in addition to the institution and respondent) could face direct personal liability for a breach of the duty of loyalty.

11. Parallel Proceedings

Be Aware of Parallel Proceedings

Proceeding	Lead	Timeline	Standard	Stakes
Institutional inquiry	RIO / committee	60 days	Preponderance	Misconduct finding
ORI oversight	ORI	Post-investigation	Deference to institution	Debarment, supervision
DOJ civil (FCA)	DOJ / USAO	Years	Preponderance	Treble damages + penalties
DOJ criminal	DOJ / FBI	Years	Beyond reasonable doubt	Imprisonment, fines
Sponsor audit	NIH / OIG	Variable	Compliance standards	Funding clawback

Operational Inquiry

What other parallel proceedings and obligations should be considered?

Questions



Attending Live?

Live Course Code #1:
Research-Live

Live Course Code #2:
Misconduct-Live

*At the end of the session, simply scan the QR code for **live** or **on-demand** session to enter the course codes.*



Attending On-Demand?

On-Demand Course
Code #1: **OD-Research**

On-Demand Course Code
#2: **OD-Misconduct**

Contact Our Presenters:



Melissa Markey

Attorney
mmarkey@hallrender.com



Rebecca Merrill

Attorney
rmerrill@hallrender.com