DUAL ENDPOINTS & THE FORGOTTEN QBE LAPTOP

OPERATIONAL SEQUENCE AT THE HEART OF THIS WHISTLEBLOWER DISPUTE

The Issue Is Not Whether Policies Existed.

The Issue Is Whether Mphasis and QBE Created, Directed, Tolerated, and Relied Upon a Dual-Endpoint Workflow While Denying Compliant Alternatives — and the QBE Laptop (an Active Endpoint to US Data) Was Left Operationally Unresolved

	WHAT HAPPENED (KEY POINTS)	MPHASIS'S ROLE / IMPACT	QBE'S ROLE / IMPACT	THE REALITY
1 WORKFLOW DIRECTION *Dual-endpoint workflow created and directed.*	• Assigned to QBE-related projects in Oct. 2024. • Requested support for deliverables including QBE PowerPoint work (ECF 14-4). • Only had access to personal Mac. • Work expected and relied upon under these conditions.	Created and directed the workflow while knowing he had no Mphasis laptop or compliant environment.	Provided a QBE-issued laptop with direct access to US systems and data but did not coordinate endpoint governance or receipt/return procedures.	Both entities established and relied on a dual-endpoint workflow without providing compliant, controlled alternatives.
2 INFRASTRUCTURE DENIAL – DUAL ENDPOINTS IMPOSED *No compliant alternative provided.*	• No Mphasis laptop provided. • "ONLY Mphasis domain joined machines" allowed. • Web-only restrictions imposed. • Repeated requests for compliant tooling denied or ignored. • Forced to operate on personal Mac + QBE laptop.	Denied compliant alternatives and imposed infrastructure limitations that created the dual-endpoint condition.	Failed to provide clear endpoint policy, inventory controls, or lifecycle management for the QBE laptop assigned to him.	Infrastructure choices by both parties forced an insecure, dual-endpoint workflow.
3 OPERATIONAL RELIANCE *Workflow continued and depended upon.*	• Deliverables continued; work product accepted. • Management visibility and ongoing communications. • Workflow continued with full knowledge of the limitations. • Dual-endpoint operation became the norm.	Operationally relied on the dual-endpoint workflow and continued to expect and accept performance.	Relied on his access to QBE systems and data without enforcing endpoint control or tracking the assigned device.	Both entities relied on and benefited from the same workflow they later attacked.
4 ESCALATIONS & DLP INCIDENT *Concerns escalated in real time.*	• "Potential DLP Incident – DR110325111903" (ECF 14-5). • Actively escalated to Mphasis security/CRO. • Explained workflow, infrastructure limits, and security concerns in real time. • Not concealed—open, contemporaneous escalation.	Was aware of the concerns, DLP escalation, and the dual-endpoint workflow through an active escalation chain.	As a direct data controller, QBE was made aware of security concerns yet took no action to secure, track, or recover its endpoint.	Clear, contemporaneous notice to both entities about unacceptable risk to US data.
5 PROTECTED COMPLAINTS *Whistleblower activity under the law.*	• Repeatedly raised cybersecurity, policy inconsistencies, governance failures, and compliance risks. • Complaints made internally to management and security/compliance. • Protected activity under SOX, Dodd-Frank, NY Labor Law § 740.	Received protected complaints about risks while continuing the same dual-endpoint workflow expectations.	Received notice of risk to its US data via the QBE laptop yet failed to take reasonable steps to secure or retrieve it.	Protected whistleblower activity was met with inaction, not remediation.
6 LATER RECHARACTERIZATION *Same workflow recast as misconduct.*	• After escalation and termination, Plaintiff characterized the same workflow as "misconduct," "unauthorized access," and "policy violations." • Filed litigation and sought injunctive relief based on that recharacterization.	Recharacterized the same operational sequence as misconduct only after protected complaints and termination.	Aligned with litigation narrative despite its own failure to manage, track, or recover the active QBE-issued laptop.	Classic retaliation and pretext: attack the messenger, not the known security failure.
7 THE FORGOTTEN QBE LAPTOP *Active endpoint to US data was left operationally unresolved.*	• After termination, the QBE laptop on his desk was left operationally unresolved. (ECF 221) • Mphasis tried to retrieve it using a private investigator — but it is not their laptop. • It took a Court Order for QBE to issue return instructions. • QBE returned the laptop to a VP, not to a fulfillment center or asset-security facility, contrary to standard practice. • The device became a central issue only after escalation and litigation.	Sought retrieval through a private investigator, but the device was not theirs. Did not ensure coordinated endpoint governance during or after separation.	Left an active endpoint to US data operationally unresolved (ECF 221) until compelled by Court Order. Returned to a VP, not through standard offboarding/secure disposition controls.	Endpoint-governance failure by both entities. Active endpoint to US data was left unresolved until after protected activity and litigation.

THE CENTRAL DISPUTE

Whether Mphasis and QBE created the dual-endpoint conditions, relied upon the resulting performance, denied compliant alternatives, and left the QBE laptop (an active endpoint to US data) operationally unresolved — only to later recharacterize the same operational sequence as misconduct after protected complaints were raised.

The Injunction Narrative Does Not Reflect the Full Operational Record.

THE RECORD REFLECTS AN ACTIVELY DISCUSSED OPERATIONAL WORKFLOW OCCURRING UNDER ENTERPRISE-CREATED INFRASTRUCTURE CONSTRAINTS, DUAL-ENDPOINT OPERATION, AND GOVERNANCE FAILURES.

This Is Not a Simplistic Policy-Violation Case — It Is a Whistleblower, Retaliation, and Pretext Dispute.