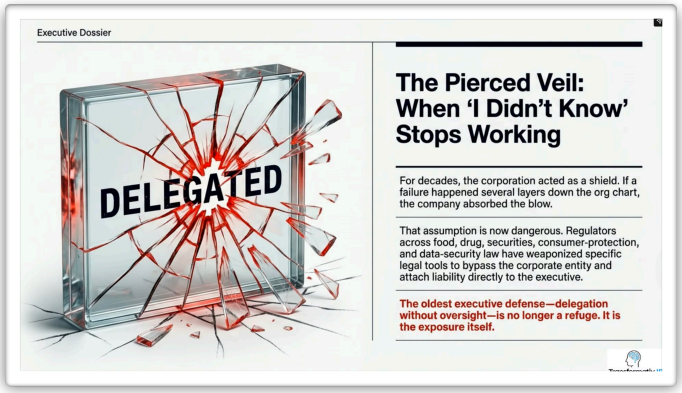
Executive Personal Liability:
The Case for Proactive Compliance
How Regulators Are Reaching Past the Company to Hold the CEO Personally Liable

A look at what the case law actually says about willful violation, willful blindness, and the shrinking corporate veil.



The two videos above outline the challenges facing the C-suite in 2026. Video 1 is a 5-minute cinematic overview, while Video 2 is a 3-minute narrated slide deck with more details.

For most of the modern corporate era, a chief executive could treat the corporation as a shield. The company signed the contracts, assumed the liability, and if something went wrong several layers down the org chart, the company — not the person at the top — absorbed the blow. That assumption is quietly becoming dangerous. Across food and drug law, environmental law, securities law, consumer-protection law, and now data security, regulators and prosecutors have been building and sharpening tools designed to do one specific thing: reach past the corporation and attach liability to the executive personally. In other words, we are entering a new legal reality where "I Didn't Know" stops working for the C-suite.

This is not a prediction. It is a pattern already written into decided cases. And the most important shift is not a single statute — it is a doctrine of mental state that has steadily dismantled the oldest executive defense of all: **"I delegated it, and I didn't know."**

The defense that no longer holds: willful blindness

Many criminal statutes require that a defendant acted "knowingly." Executives have long assumed this protects them — that if bad news never reached their desk, they could not have "known," and therefore could not be guilty. Courts closed that escape hatch with the **willful blindness** doctrine (also called conscious avoidance or, more colorfully, the "ostrich defense").

The Supreme Court fixed the modern standard in re ***Global-Tech Appliances, Inc. v. SEB S.A.*** (2011). Under its two-part test, a person is treated as having actual knowledge when they:

(1) subjectively believe there is a high probability that a fact exists, and

(2) take deliberate steps to avoid confirming it.

In plain terms: if you suspect something is wrong and you arrange not to find out, the law treats you as if you knew.

The Court was careful to keep this distinct from mere carelessness — negligence is not enough — but the bar it set is one a busy executive can cross simply by looking away from red flags.

The practical consequence is stark. An executive who structures the organization so that uncomfortable facts never arrive has not built a defense; under this doctrine, that very arrangement can become the evidence of a guilty mind. Delegation without oversight is no longer a refuge. It is increasingly the exposure itself.

Where executives already go to prison without proof that they knew

In a category of "public welfare" offenses — food, drugs, and the environment — the law goes even further than willful blindness. Under the **Responsible Corporate Officer (RCO) doctrine**, also known as the **Park doctrine**, a senior officer can be convicted of a crime without any proof that they participated in, ordered, or even knew about the violation. Liability attaches to the officer's position and authority — specifically, the power to prevent or promptly correct the violation, and the failure to do so.

The doctrine traces to two Supreme Court decisions, ***United States v. Dotterweich*** (1943) and ***United States v. Park*** (1975). In ***Park***, the CEO of a national supermarket chain was held criminally responsible for unsanitary, rodent-infested warehouse conditions he had not personally created and had delegated to subordinates to fix. The fine was trivial; the precedent was not. The Court held that those who voluntarily assume positions of authority over enterprises affecting public health accept a duty of foresight and vigilance — and can be punished when they fail it.

For decades, the doctrine produced fines rather than prison, but that has changed:

- *In re* ***United States v. DeCoster*** (8th Cir. 2016; cert. denied 2017). After a nationwide salmonella outbreak traced to their egg operation, owner Austin "Jack" DeCoster and his son Peter were each sentenced to three months in federal prison — upheld on appeal — despite the absence of evidence that either personally knew their eggs were contaminated. Their positions of authority were enough.
- *In re* ***United States v. Huggins (Synthes/Norian)*** (2011). Four executives of the medical-device maker Synthes pleaded guilty to misdemeanor misbranding charges tied to unauthorized clinical use of a bone cement the FDA had warned against. Michael Huggins, President of Synthes North America, received nine months in prison; others received five to nine months. They are widely regarded as among the first executives actually imprisoned under the ***Park*** doctrine — punished as responsible officers, not as people proven to have personally committed the underlying acts.
- *In re* ***United States v. Hong*** (4th Cir. 2001). An executive who effectively controlled a wastewater company was held criminally liable under the Clean Water Act for discharges he did not personally perform and was sentenced to three years in prison. The court confirmed that a responsible officer's authority over the offending operation — not hands-on involvement — is what matters.

A crucial caveat, and one worth stating plainly because sophisticated readers will test for it: the ***Park*** doctrine lives in public-welfare law. Specifically, the regulatory and judicial mindset behind it — that authority carries non-delegable accountability — is now migrating into other fields through different legal vehicles.

The doctrine crosses into data and cybersecurity

Because cybersecurity is not a traditional public-welfare statute, prosecutors pursuing technology executives have reached for other tools — fraud, obstruction, and securities law — and they have started to win.

- The landmark is ***United States v. Sullivan***. Joseph Sullivan, the Chief Security Officer of Uber, was convicted in 2022 of obstruction of justice and misprision of a felony for concealing a 2016 data breach from the Federal Trade Commission while the agency was actively investigating the company — a concealment carried out by routing a payment to the hackers through a bug-bounty program and securing non-disclosure agreements.
    - On March 13, 2025, the Ninth Circuit unanimously affirmed the conviction. Sullivan received three years of probation and a $50,000 fine, but the precedent is the point: a security executive was held personally, criminally responsible for how he handled a breach. The court noted, pointedly, that transparency matters most precisely when a failure is already under federal investigation.
- Regulators have pushed even harder on the civil side, with mixed results that are worth reporting honestly. In re ***SEC v. SolarWinds Corp. and Timothy G. Brown*** (2023), the Securities and Exchange Commission took the rare step of charging a sitting CISO personally with fraud over allegedly misleading statements about the company's cybersecurity. In July 2024, a federal judge dismissed most of those claims, allowing only a narrow set to proceed. Cited in full, the case makes a more credible point than cherry-picking either half: regulators are now willing to name individual security executives — and courts will still police the limits of how far that can go. The direction of travel is unmistakable even where the courts apply the brakes.

When the penalty follows the person, not the company

Perhaps the most underappreciated shift is civil, not criminal. The FTC has increasingly written orders that bind the executive as an individual — obligations that travel with them to whatever company they run next, long after they've left the one where the failure occurred.

In re ***Drizly, LLC and James Cory Rellas*** (FTC 2022), the Commission named the CEO personally and imposed security obligations that attach to him at future companies, not just the one breached — a deliberate signal that an executive cannot simply walk away from a security failure by changing employers. In re ***InfoTrax Systems, L.C. and Mark Rawlins*** (finalized 2020), the order bound the former CEO personally and required ongoing, independent third-party security assessments. And in re ***Support King, LLC (SpyFone) and Scott Zuckerman*** (FTC 2021), the Commission banned the CEO outright from the surveillance-and-monitoring industry — a personal, field-specific exile, not merely a corporate fine.

These orders convert a one-time corporate settlement into a long-term personal mandate. For an executive, that is a different category of risk: it touches future employability, future fundraising, and personal reputation in a way no corporate penalty does.

The securities overlay: certifications, clawbacks, and the federal gap

Securities law adds another layer aimed squarely at the top of the house. Under the Sarbanes-Oxley Act, CEOs and CFOs must personally certify their financial reports.

- **A knowing false certification under Section 906 carries up to ten years in prison; a willful one carries up to twenty years in prison.**
- **Signing as a routine formality is not a defense — prosecutors treat unreviewed certification as exactly the kind of conscious avoidance that satisfies criminal intent.**

- **Section 304 lets the SEC claw back a CEO's bonus and incentive pay after a misconduct-driven restatement, *even when the executive engaged in no misconduct personally.***

There is also a gap that catches executives by surprise. Under Delaware's ***Caremark*** and ***Stone v. Ritter*** line of cases, the bar for personal oversight liability in civil corporate law is famously high — generally requiring a near-total failure to even attempt oversight. Many executives take comfort there. But federal prosecutors, guided by the policy lineage of the DOJ's individual-accountability memoranda, apply a far more demanding standard. An oversight program that comfortably clears the Delaware bar can still be viewed federally as a "paper" system — evidence of structured ignorance rather than genuine control.

Why is this sharper now than a year ago

Three developments have widened the statutory surface area in just the past two years, and each one carries the language of personal and willful liability.

1. First, the Department of Justice's **Data Security Program**, which took effect April 8, 2025, under Executive Order 14117, restricts bulk transfers of Americans' sensitive personal data to designated countries of concern.
    a. It is enforced under the International Emergency Economic Powers Act, and **willful violations can carry criminal penalties of up to twenty years in prison and a $1 million fine.**
    b. Critically, it extends to ordinary vendor, employment, and investment arrangements, not just data brokers, so mid-sized companies can fall within its scope without realizing it.
2. Second, the state privacy-law wave is now real and enforced. **Roughly twenty states have comprehensive privacy laws in effect as of 2026, with new requirements around risk assessments, automated decision-making, and security audits coming online, and state attorneys general have moved from warning letters to active enforcement.**
3. Third, the SEC's cybersecurity disclosure rules **now require public companies to disclose material incidents within four business days** — a clock that turns a quiet, mishandled breach into a potential securities problem with remarkable speed.

Layered onto the willful blindness doctrine, these regimes share a common feature: they punish *willfulness* and *deliberate avoidance* more harshly than honest failure. The executive who can show genuine, documented, continuous oversight is in a fundamentally different position from the one who arranged not to look.

The throughline — and the prudent response

Read together, these cases tell a single coherent story. The willful blindness doctrine has erased the gap between "I didn't know" and "I should have known and chose not to." The ***Park*** line shows that authority alone can carry criminal accountability. ***Sullivan*** shows the principle has reached cybersecurity. **The FTC's individual orders show the penalty can follow the person for decades. And the newest data-security and privacy regimes show the trend accelerating, with willful-violation penalties written directly into the statutes.**

The honest conclusion is not that every CEO is one breach away from prison. It is narrower and more useful: the legal system increasingly distinguishes between executives who maintained real, demonstrable oversight and those who didn't — and it punishes the second group with tools aimed at the individual. In that environment, proactive compliance is not an administrative cost or an act of fear. It is the single most reliable way to convert "I didn't know" into something the law actually respects: "I built a system to know, I can prove it, and I acted on what it told me."

That is the difference between willful blindness and responsible oversight — and, increasingly, it is the difference the cases turn on. The prudent executive does not wait to learn which side of that line they are on. They build the documentation now, while it is still a choice rather than a defense.

This article is provided for general informational purposes and reflects publicly reported cases and regulations as of 2026. It is not legal advice and does not create an attorney-client relationship. Case outcomes, sentences, and regulatory rules can change and turn on specific facts; consult qualified legal counsel about your organization's particular situation.

PQC+™

Transformativ IP

Regulatory Compliance and HNDL Protection
Federal and 50 States within 90 Days