IN THE UNITED STATES COURT OF FEDERAL CLAIMS

THEODORE HAUGLAND,
Plaintiff,

V.

THE UNITED STATES OF AMERICA,
Defendant

Case No: 1:25-CV-01744-EDK
Judge: Elaine D. Kaplan

PLAINTIFF'S MOTION FOR PROTECTIVE ORDER

Plaintiff respectfully moves this Court, pursuant to Rule 26(c) of the Rules of the United States Court of Federal Claims ("RCFC") and Appendix C, for entry of a Protective Order governing the handling of confidential, competition-sensitive, and tax-return information in this matter. This motion is prompted by the August 2025 breach of the judiciary's Case Management/Electronic Case Files ("CM/ECF") system, which exposed vulnerabilities affecting sealed and restricted filings. Plaintiff anticipates that discovery and filings in this case will encompass information protected under 26 U.S.C. §§ 6103, 7431, and other federal confidentiality statutes.

I. INTRODUCTION

This litigation will require production and filing of sensitive taxpayer information, proprietary business records, internal pricing analyses, and other confidential materials. The 2025 CM/ECF breach demonstrates that the judiciary's electronic filing systems have been, and remain, vulnerable to unauthorized access—even when documents are filed under seal.

Disclosure of such information would cause irreparable harm, including:

- Unauthorized dissemination of Plaintiff's tax returns and private financial data;
- Exposure of proprietary pricing, bidding, and strategic business information;
- Violations of statutory confidentiality under 26 U.S.C. § 6103;
- Potential liability and damages under 26 U.S.C. § 7431; and
- Permanent competitive and privacy harm that cannot be cured.

Given these risks and the repeated systemic failures described below, Plaintiff seeks heightened protections beyond the standard model Protective Order in Appendix C.

II. LEGAL STANDARD – RCFC 26(c)

RCFC 26(c) authorizes courts to issue protective orders "for good cause," including measures preventing disclosure of trade secrets or confidential commercial, financial, or research information. Courts routinely issue protective orders where disclosure could create competitive harm or violate statutory confidentiality.

See, e.g.:
- *Genentech, Inc. v. Trustees of Univ. of Penn.*, 2008 WL 11449565 (Fed. Cl. 2008);
- *United States v. Microsoft Corp.*, 165 F.3d 952, 959 (D.C. Cir. 1999);
- *United States v. Pomponio*, 429 U.S. 10, 12 (1976);
- 26 U.S.C. §§ 6103, 7431.

A protective order is necessary to maintain the integrity of sealed proceedings, to comply with federal tax-confidentiality statutes, and to mitigate risks presented by the demonstrated vulnerabilities of CM/ECF.

III. FACTUAL BASIS – 2025 CM/ECF DATA BREACH

In August 2025, the judiciary publicly acknowledged a breach of its CM/ECF system, revealing that sealed filings had been accessed by unauthorized parties. The consequences included:

- Court instructions limiting electronic filing of highly sensitive documents;
- Notices advising litigants to review filing procedures for sealed materials;
- Federal agencies initiating audits of sealed-document protocols.

This event confirms that filing materials under seal is not, by itself, sufficient protection. Enhanced protective procedures are required to safeguard Plaintiff's statutorily protected information.

III-A. GROUNDS FOR PROTECTIVE ORDER – LONGSTANDING SYSTEMIC VULNERABILITIES

The July–August 2025 breach was the predictable result of a documented pattern of unaddressed CM/ECF vulnerabilities:

A. SolarWinds Compromise (2020–2021)

In 2020, the judiciary suspended use of SolarWinds products after confirming an "apparent compromise" of CM/ECF. Parties were directed to file highly sensitive documents on paper due to insecure electronic systems.

B. Congressional Findings (2021)

Congressional investigations concluded that the 2021 breach exposed sealed filings and that CM/ECF security was seriously deficient. Despite this, no comprehensive modernization occurred.

C. Government-Wide Cybersecurity Failures (2020)

While other federal agencies implemented sweeping defensive reforms, the judiciary did not adopt comparable safeguards for CM/ECF.

D. Expert Warnings (2021–2025)

Cybersecurity specialists repeatedly cautioned that CM/ECF was outdated and vulnerable. Legal and cybersecurity analysts described the system as a "stark warning" for litigants required to file confidential information.

E. Judicial Conference Testimony (2025)

On June 26, 2025, Judge Michael Scudder, Chair of the Judicial Conference IT Committee, testified that CM/ECF was "unsustainable," "outdated," and "at risk of operational failure or security breaches," specifically noting that sealed filings had already been targeted.

+-F. Continued Failure to Implement Safeguards

Despite widespread, years-long warnings, CM/ECF remained insecure, culminating in the 2025 breach that exposed sealed filings such as Plaintiff's. This history further demonstrates the need for heightened protective measures.

IV. NEED TO PROTECT TAX-RETURN INFORMATION

Discovery will require production of Plaintiff's tax returns, financial records, and internal analyses. Unauthorized disclosure would:

- Violate the tax-confidentiality protections of 26 U.S.C. § 6103;
- Create liability under 26 U.S.C. § 7431;
- Irreparably harm Plaintiff's competitive standing;
- Undermine trust in the confidentiality of sealed judicial filings.

Courts consistently recognize the need for heightened protection of tax-return information. See *United States v. BDO Seidman, LLP*, 492 F.3d 806 (7th Cir. 2007); *United States v. Reynolds*, 345 U.S. 1 (1953); *In re Sealed Case*, 838 F.2d 476 (D.C. Cir. 1988).

V. PROPOSED PROTECTIVE ORDER

Plaintiff respectfully requests entry of the following Protective Order to safeguard confidential, competition-sensitive, taxpayer, and statutorily protected information during litigation:

I. Protected Information and Use

Definition: "Protected information" includes any confidential, proprietary, trade-secret, competition-sensitive, or tax-return information, whether contained in documents, ESI, deposition testimony, or declarations.

Use Restrictions: Protected information may be used solely for purposes of this litigation and may not be disclosed except as authorized by this Order or federal law.

II. Access to Protected Information

Authorized access is limited to:
- Counsel of record;
- Independent experts/consultants;
- Court personnel;
- DOJ and relevant agency personnel.

Access requests shall be made using Appendix C Form 9 (counsel) or Form 10 (expert/witness). Objections must be filed within two business days.

III. Identification and Filing Requirements

Electronic filings: "CONTAINS PROTECTED INFORMATION" must appear in the subject line and caption.
Paper filings: Must be sealed and prominently marked as containing protected information.

IV. Redactions

Parties shall serve a "Proposed Redacted Version." Additional redactions must be proposed within two business days. Disputes will be resolved by the Court.

V. Safeguarding, Breach Response, and Remedies

- No more than three copies may be made absent consent or Court order.
- Individuals must securely store protected information.
- **Breach Notification:** Any unauthorized disclosure must be reported immediately to opposing counsel and the Court, with steps taken to mitigate and recover the information.
- The Court may grant appropriate relief for violations.

VI. Retention and Disposal

Following final judgment, protected materials must be destroyed or returned within 30 days, except copies retained as required by law. The Court will maintain sealed records under RCFC 77.4(c).

VI. TABLE OF AUTHORITIES

Statutes
26 U.S.C. § 6103
26 U.S.C. § 7431

Rules
RCFC 26(c)
RCFC Appendix C

Cases
Genentech, Inc. v. Trustees of Univ. of Penn., 2008 WL 11449565 (Fed. Cl. 2008)
United States v. Microsoft Corp., 165 F.3d 952 (D.C. Cir. 1999)
United States v. Pomponio, 429 U.S. 10 (1976)
United States v. BDO Seidman, LLP, 492 F.3d 806 (7th Cir. 2007)
United States v. Reynolds, 345 U.S. 1 (1953)
In re Sealed Case, 838 F.2d 476 (D.C. Cir. 1988)

VII. CASE LAW SUPPORTING ENTRY OF A PROTECTIVE ORDER FOLLOWING DATA BREACH

Beyond the statutory and factual grounds described above, substantial precedent from the Supreme Court, Federal Circuit, Court of Federal Claims, and persuasive federal authority recognizes courts' responsibility to protect sensitive, confidential, proprietary, and statutorily protected information through sealing orders and tailored protective orders. These authorities strongly support granting Plaintiff's requested enhanced protections.

A. Supreme Court Precedent Recognizing Protection of Confidential Information

1. Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984)

The Supreme Court confirmed that courts have broad discretion to issue protective orders where needed to protect privacy and confidential information and held that "pretrial discovery… may seriously implicate privacy interests." Id. at 34–36.
This case provides foundational authority that courts may, for good cause, restrict dissemination of discovery materials—even absent a First Amendment right—where the information is sensitive or private.

2. United States v. Reynolds, 345 U.S. 1, 7–8 (1953)

Reynolds recognizes that courts may protect confidential or sensitive information to prevent harm or unauthorized disclosure. Although arising in the context of military secrets, the Court confirmed that federal courts possess inherent authority to restrict disclosure of information that could compromise privacy, confidential interests, or governmental obligations.

3. Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978)

The Court recognized that access to judicial records is not absolute and may be overridden where disclosure would result in improper use of confidential information, trade secrets, or sources of business information. Id. at 598.

These principles support stronger protection for Plaintiff's tax-return information, proprietary business data, and other confidential records at risk due to CM/ECF vulnerabilities.

B. Federal Circuit and Court of Federal Claims Precedent Requiring Protection of Proprietary, Competition-Sensitive, and Confidential Information

1. U.S. Court of Appeals for the Federal Circuit

Apple Inc. v. Samsung Elecs. Co., 727 F.3d 1214, 1221 (Fed. Cir. 2013)

The Federal Circuit held that courts must protect sensitive business information where disclosure threatens competitive harm. The decision confirms that such information qualifies as protectable under sealing and protective orders.

In re Violation of Rule 28(d), 635 F.3d 1352 (Fed. Cir. 2011)

The court reaffirmed that confidential information—including trade secrets, financial records, and proprietary data—merits protection from public disclosure.

These decisions confirm that competition-sensitive information like Plaintiff's pricing and financial data warrants protective treatment.

---

2. Court of Federal Claims

Genentech, Inc. v. Trustees of Univ. of Penn., 2008 WL 11449565 (Fed. Cl. 2008)

The Court of Federal Claims granted heightened protective measures to safeguard research, proprietary data, and confidential commercial information—supporting the proposition that RCFC 26(c) demands protection where competitive harm is possible.

Ammex, Inc. v. United States, 2018 WL 4705790 (Fed. Cl. 2018)

The court held that protecting proprietary financial information is appropriate because disclosure "could provide an unfair competitive advantage."

Uusi, LLC v. United States, 110 Fed. Cl. 604, 612 (2013)

The court noted that RCFC 26(c) authorizes restrictions to prevent undue exposure of confidential commercial information and emphasized that courts should grant protective orders when necessary to secure private data.

C. Federal Authority Supporting Protection of Taxpayer and Financial Information

1. United States v. BDO Seidman, LLP, 492 F.3d 806 (7th Cir. 2007)

The Seventh Circuit held that taxpayer and financial materials warrant protected status, reaffirming that courts must shield documents implicating confidential tax-return information.

2. Gardner v. United States, 213 F.3d 735 (D.C. Cir. 2000)

The court reaffirmed the strict confidentiality protections of 26 U.S.C. § 6103 and emphasized that even inadvertent disclosures of tax-return information constitute violations.

3. In re Sealed Case, 838 F.2d 476 (D.C. Cir. 1988)

This case further stresses that courts must carefully preserve statutory confidentiality safeguards in civil proceedings.

These authorities underscore the necessity of enhanced protective measures where, as here, § 6103 and § 7431 confidentiality obligations are directly implicated.

D. Authority Addressing the Risks of Electronic Systems and Data Breaches

Federal courts increasingly recognize the need for heightened protections when electronic systems are vulnerable:

1. In re Sony Gaming Networks Data Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014)

The court held that cybersecurity vulnerabilities justify measures to prevent further unauthorized disclosure and recognized that failure to safeguard confidential information causes ongoing harm.

2. Doe v. Luzerne County, 660 F.3d 169, 175 (3d Cir. 2011)

The court recognized an individual constitutional privacy interest in preventing dissemination of confidential personal data, reinforcing that courts must act to prevent exposure through electronic systems.

These cases bolster the argument that the judiciary's known cybersecurity vulnerabilities justify heightened protective measures to prevent further disclosure of sensitive Plaintiff information.

E. Courts' Inherent Authority to Protect the Integrity of the Judicial Process

Federal courts possess inherent power to "manage their own affairs so as to achieve the orderly and expeditious disposition of cases."
See *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43 (1991).

This includes authority to issue protective orders to:
- safeguard confidential filings,
- remedy or mitigate data breaches, and
- preserve litigants' trust in the judicial process.

Given the judiciary's acknowledged CM/ECF failures, exercising this inherent authority is necessary to protect Plaintiff from further harm.

VIII. CONCLUSION

For all the factual, statutory, and judicial reasons set forth in Sections I–VIII, Plaintiff respectfully requests that the Court:

1. **Enter the heightened Protective Order** proposed herein;
2. Recognize that longstanding CM/ECF vulnerabilities—affirmed by courts, Congress, cybersecurity experts, and the Judicial Conference—necessitate enhanced safeguards;
3. Ensure compliance with 26 U.S.C. §§ 6103 and 7431 and other legal confidentiality obligations; and
4. Protect Plaintiff's financial, tax-return, and proprietary business information from further unauthorized exposure.

Respectfully Submitted,

December 12, 2025
Date

/s/ Theodore Haugland
THEODORE HAUGLAND
Plaintiff, *Pro Se*
99-009 Kalaloa St
Unit D2016
Aiea, HI 96701
United States
(202)933-3332
theodorehaugland@outlook.com
Case 1:25-cv-01744-EDK

THEODORE HAUGLAND
99-009 KALALOA ST
STE D2016
AIEA, HI 96701

UNITED STATES COURT OF FEDERAL CLAIMS
ATTENTION: COURT CLERK
717 MADISON PL, NW
WASHINGTON, DC 20439-0001

USPS FIRST-CLASS MAIL®
US POSTAGE IMI 059251212145021 2000394174
$8.30
SSK
FCM
12/12/25 Mailed from 96820 028W2311275
THEODORE HAUGLAND
D2016
KALALOA ST
96701-3498
5.30 oz
RDC 99
COURT CLERK
USCFC
WASHINGTON DC 20439
USPS CERTIFIED MAIL®
9507 1067 1411 5346 3364 02

In the United States Court of Federal Claims

THEODORE HAUGLAND
Plaintiff(s),

v.

THE UNITED STATES,

Defendant.

Case No. 1:25-CV-01744-EDK

Judge Elaine D. Kaplan

CERTIFICATE OF SERVICE

I hereby certify that on December 12, 2025, _____, a copy of plaintiffs motion for protective order, was mailed via USPS Certified Mail, to Eric J. Smith, at PO Box 26, Washington, DC 20530.

Theodore Haugland
(Signature of Applicant)

Theodore Haugland
(Printed Name)

99-009 Kalaloa St # D2016
(Street Address)

Aiea, HI 96701
(City, State, ZIP Code)

(202)933-3332
(Phone Number)

THEODORE HAUGLAND
99-009 KALALOA ST
STE D2016
AIEA, HI 96701

UNITED STATES COURT OF FEDERAL CLAIMS
ATTENTION: COURT CLERK
717 MADISON PL, NW
WASHINGTON, DC 20439-0001