

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

KENNETH C. GRIFFIN,

Plaintiff,

v.

INTERNAL REVENUE SERVICE and U.S.
DEPARTMENT OF THE TREASURY,

Defendants.

Case No.

Jury Trial Demanded

COMPLAINT

Plaintiff Kenneth C. Griffin (“Mr. Griffin”), by and through his undersigned counsel, brings this action against the Internal Revenue Service (“IRS”) and the U.S. Department of Treasury (collectively, “Defendants”) to seek redress for the IRS’s unlawful disclosure of Mr. Griffin’s confidential tax return information in violation of 26 U.S.C. § 6103 and Defendants’ violation of the Privacy Act, 5 U.S.C. § 552a, for their willful and intentional failure to establish appropriate administrative, technical, and/or physical safeguards over its records system to insure the security and confidentiality of Mr. Griffin’s confidential tax return information.

1. Mr. Griffin, a self-made entrepreneur and investor, is the founder and Chief Executive Officer of Citadel, a global alternative investment firm, and a founder and the non-Executive Chairman of Citadel Securities, a leading global market maker. He is proud of his success and has always sought to pay his fair share of taxes. Indeed, Mr. Griffin apparently pays federal income taxes at a higher effective tax rate than many of the top wage earners in the United States.¹

¹ ProPublica, *America’s Top 15 Earners and What They Reveal About the U.S. Tax System*,

2. Mr. Griffin has complied with the IRS's annual requirements to report his personal and confidential financial information, and he did so—like virtually all Americans—believing that the IRS would comply with its own legal obligations to safeguard and protect his information from unauthorized disclosure, as required by Section 6103 of the Internal Revenue Code as well as the Privacy Act, 5 U.S.C. § 552a.

3. On information and belief, in or after 2019, IRS personnel exploited the IRS's willful failure to establish adequate administrative, technical, and physical safeguards for the IRS's data and records systems to misappropriate confidential tax return information for the highest earning U.S. taxpayers, including Mr. Griffin, and then unlawfully disclosed those materials to ProPublica for publication.

4. Indeed, in or around March 2022, Mr. Griffin learned that ProPublica had acquired the confidential tax return information that Mr. Griffin reported to the IRS, along with the confidential tax return information “of thousands of the nation’s wealthiest people, covering more than 15 years.”² ProPublica boasted that the information it obtained was “not just tax returns,” but also included “information that is sent to the IRS about financial activities” such as “income and taxes,” “investments, stock trades, gambling winnings and even the results of audits.”³ Significantly, ProPublica identified the IRS as the source of the confidential information it

PROPUBLICA, April 13, 2022, <https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system>.

² Jesse Eisinger, Jeff Ernsthause & Paul Kiel, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, PROPUBLICA, June 8, 2021, <https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax>.

³ ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, <https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files>.

published, including Mr. Griffin's return information.

5. Mr. Griffin learned that ProPublica intended to publish a story "about the highest earning Americans, in which [ProPublica] plan[ned] to mention several dozen people including [Mr.] Griffin," as well as another story contrasting the relatively high effective income tax rate that Mr. Griffin pays with the apparently lower effective tax rate paid by the CEO of one of Citadel Securities' commercial competitors.

6. On April 13, 2022 and on July 7, 2022, ProPublica published confidential tax return information regarding Mr. Griffin's 2013-2018 federal income tax years, including Mr. Griffin's purported average annual income, purported percent of income deducted, and purported average effective federal income tax rate for those periods.⁴ In publishing the information, ProPublica acknowledged that it was the confidential tax return information of "people who, in good faith, sent their tax and personal and private information to the Internal Revenue Service with no expectation that it would ever be made public."⁵

7. Over the past year, ProPublica has continued to publish more and more confidential tax return information of the taxpayers targeted by its articles, and it is clear why Mr. Griffin's and these other taxpayers' confidential tax return information was and may continue to be so readily available to ProPublica: the IRS's well known, systemic failures to establish appropriate safeguards to protect taxpayers' confidential return information from unauthorized and unlawful

⁴ Paul Kiel & Mick Dumke, *Ken Griffin Spent \$54 Million Fighting a Tax Increase for the Rich. Secret IRS Data Shows It Paid Off for Him*, PROPUBLICA, June 7, 2022, <https://www.propublica.org/article/ken-griffin-illinois-graduated-income-tax>; ProPublica, *America's Top 15 Earners and What They Reveal About the U.S. Tax System*, PROPUBLICA, April 13, 2022, <https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system>.

⁵ ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, <https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files>.

inspection and disclosure.

8. Federal agencies depend on information technology systems and electronic data to carry out operations and to process, maintain, and report essential information. Every year from fiscal year 2010 through 2020, however, the Treasury Inspector General for Tax Administration (“TIGTA”) has put the IRS on notice that deficiencies in its “Security Over Taxpayer Data and Protection of IRS Resources” were the IRS’s “number one major management and performance challenge area.”⁶

9. Despite annual audits, TIGTA—for more than a decade—continued to find systemic failures by the IRS to establish appropriate administrative, technical, and physical safeguards to adequately protect the unlawful disclosure of taxpayers’ confidential tax return information. For example, in its *Annual Assessment of the IRS’s Information Technology Program for Fiscal Year 2020*, TIGTA revealed that the IRS failed to use “encryption algorithms” in accordance with the Federal Processing Standards 140-2, *Security Requirements for Cryptographic Modules* for certain operating systems in order to keep confidential tax return information “unreadable for an unauthorized user.”⁷ Likewise, TIGTA reported that 2 out of 5 of the IRS’s Cybersecurity Framework functions (*i.e.*, Identify, Protect, Detect, Respond, Recover) “were deemed as ‘not effective.’”⁸ TIGTA also identified myriad security deficiencies for the IRS system that collects, converts, and stores a taxpayer’s confidential tax return information into

⁶ See TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2021-20-001, ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE’S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2020, at 6 (October 2020).

⁷ See *id.* at 22.

⁸ See *id.* at 9.

electronic records of taxpayer data,⁹ including “more than 16,000 policy violations.”¹⁰ In other instances, “the IRS inappropriately assigned business role accounts to an administrator group, resulting in those accounts [and thus inappropriate employees] having unnecessarily elevated privileges.”¹¹ Notably, TIGTA found that the IRS “lacked management oversight to insure that Federal and [Internal Revenue Manual] requirements are met” and, in “critical areas” housing computer rooms, “the IRS cannot control the movement of individuals and eliminate unnecessary traffic throughout this critical security area [to] reduce the opportunity for unauthorized disclosure or theft of tax information.”¹²

10. The IRS is and has for some time been well aware of these issues, including the unlawful disclosure of Mr. Griffin’s confidential tax return information at issue in this lawsuit. As recently as April 18, 2022, members of Congress confirmed that there “is little doubt” that the confidential tax return information disclosed to ProPublica, including Mr. Griffin’s confidential tax return information, “came from inside the IRS” and that the disclosure was “precisely what 26 U.S.C. § 6103 and related statutes were designed to prevent—the disclosure of private tax information and the political weaponization of that information.”¹³

11. Despite these warnings, however, the IRS continues to willfully and intentionally fail to establish adequate safeguards to protect Mr. Griffin and other taxpayers’ confidential tax

⁹ TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2020-20-006, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT, at 1-2 (February 2020).

¹⁰ *Id.* at *Highlights*.

¹¹ *Id.*

¹² *Id.* at 6.

¹³ Letter from Congressman Kevin Brady and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf.

return information. For example, “the IRS continues cloud deployments [that contain taxpayer data] despite not having a fully implemented security control infrastructure in place.”¹⁴ In so doing, the “IRS implemented cloud services with known capability gaps that remain in the areas of identity and access management, continuous security monitoring, data and infrastructure protection, and program management and integration.”¹⁵ In other instances, even when the IRS agreed with TIGTA recommendations to take corrective actions and perform database vulnerability scanning enterprise-wide by 2016, “the IRS made an executive decision, without following proper procedures or policy, to reduce vulnerability scanning of databases.”¹⁶ What is more, the IRS concealed its decision until TIGTA started a review in November 2020, at which time “the IRS officially announced the reduction in database vulnerability scanning, three years after it had actually reduced database vulnerability scanning.”¹⁷ Although computer mainframes are considered High Value Assets, the “IRS has not performed database vulnerability scanning on [its] International Business Machines (IBM) mainframes since 2018,”¹⁸ and according to TIGTA, “the IRS is not timely patching database vulnerabilities.”¹⁹

12. Over the past year, members of Congress have repeatedly demanded information

¹⁴ TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-052, CLOUD SERVICES WERE IMPLEMENTED WITHOUT KEY SECURITY CONTROLS, PLACING TAXPAYER DATA AT RISK, at *Highlights* (September 27, 2022).

¹⁵ *Id.* at 6.

¹⁶ TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-065, THE IRS NEEDS TO IMPROVE ITS DATABASE VULNERABILITY SCANNING AND PATCHING CONTROLS, at *Highlights*, 3 (September 30, 2022).

¹⁷ *Id.* at 4.

¹⁸ *Id.* at 4-6.

¹⁹ *Id.* at *Highlights*.

regarding how the IRS and the Treasury Department allowed the unlawful disclosures to happen.²⁰ For example, members of the House Ways and Means Committee sent letters on June 9, 2021, June 11, 2021, June 17, 2021, April 18, 2022, and October 27, 2022 to Treasury Secretary Janet Yellen, IRS Commissioner Charles Rettig, Treasury Inspector General for Tax Administration J. Russell George, and/or Acting Inspector General for the U.S. Department of Treasury Richard Delmar, and also asked questions at hearings on June 17, 2021 and June 8, 2022, all to obtain information “about the actions that led to the massive leak of private taxpayer information in June 2021 to ProPublica.”²¹ Despite admitting that the IRS’s unlawful disclosures have been “very damaging,” as recently as May 10, 2022, Treasury Secretary Janet Yellen continued to claim that she has “not seen any information on what is being found.”²² Although officials throughout the government emphasized that the conduct at issue is potentially criminal,²³ by refusing to provide

²⁰ See, e.g., Letter from Congressman Kevin Brady and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf; see also *The Financial Stability Oversight Council Annual Report to Congress: Hearing Before the S. Banking Comm.* (May 10, 2022), <https://www.youtube.com/watch?v=ObS-QV0OEw>, at approximately 1:29.

²¹ See Letter from Congresspeople Kevin Brady, Jodey Arrington, and David Kustoff, to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (October 27, 2022), <https://gop-waysandmeans.house.gov/wp-content/uploads/2022/10/10.27.22-ProPublica-Leak-Letter.pdf>.

²² *The Financial Stability Oversight Council Annual Report to Congress: Hearing Before the S. Banking Comm.* (May 10, 2022), <https://www.youtube.com/watch?v=ObS-QV0OEw>, at approximately 1:29

²³ Attorney General Merrick Garland promised that investigating the source of the IRS leak “will be at the top of my list,” IRS Commissioner Charles Rettig stated that the people involved would “absolutely” face prosecution, and Treasury Secretary Janet Yellen said that the IRS leak posed “a very serious situation, and I and the Treasury Department take very seriously the protection of government data.” Tucker Higgins, *Attorney General Garland Vows Billionaire Tax Leak To ProPublica Will Be ‘Top Of My List’ To Investigate*, CNBC, June 9, 2021, <https://www.cnbc.com/2021/06/09/propublica-tax-leak-investigation-will-be-priority-attorney-general-garland-says.html>; see also Sarah Hansen, *IRS Commissioner Warns Of Prosecution If*

Congress and/or Mr. Griffin any information on what is known and what has been done to address the IRS's unlawful disclosures, Defendants continue to obscure the IRS's failure to establish appropriate administrative, technical, and physical safeguards over its systems of records that contain taxpayers' confidential tax return information.

13. In July 2022 and again in August 2022, Mr. Griffin requested that Defendants "send a formal demand to ProPublica to return (and destroy any copies therewith) all of the confidential IRS data ProPublica has in its possession, custody, or control," and further requested Defendants provide Mr. Griffin information relevant to the unlawful disclosure of his own confidential tax return information to ProPublica. Despite Mr. Griffin's repeated requests that Defendants take at least these basic actions to help militate against further use and disclosures of Mr. Griffin's (and others') confidential tax return information, no Defendant has provided any meaningful response to Mr. Griffin's requests.

14. In enacting 26 U.S.C. §§ 6103 and 7431, as well as 5 U.S.C. § 552a(e)(10), Congress unequivocally declared its intent to safeguard the confidentiality of U.S. taxpayers' tax return information, including Mr. Griffin's confidential tax return information, and to hold the IRS to account for failing to adequately do so. By this lawsuit, Mr. Griffin respectfully requests that the Court provide damages and injunctive relief to enforce Congress's promise.

Bombshell Tax Records Were Leaked Illegally To ProPublica, FORBES, June 8, 2021, <https://www.forbes.com/sites/sarahhansen/2021/06/08/irs-commissioner-warns-of-prosecution-if-bombshell-tax-records-were-leaked-illegally-to-propublica/?sh=5bce49724aa8>; Naomi Jagoda, *Yellen: Disclosure Of Tax Data To ProPublica A 'Very Serious Situation'*, THE HILL, June 16, 2021, <https://thehill.com/policy/finance/558720-yellen-disclosure-of-tax-data-to-propublica-a-very-serious-situation/?rl=1>.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1340, 1346, 26 U.S.C. § 7431(a), and 5 U.S.C. § 552a(g)(1)(D).

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1402 because Mr. Griffin resides in this judicial district.

THE PARTIES²⁴

17. Plaintiff Kenneth C. Griffin is a citizen of the United States and a resident of Miami, Florida.

18. Defendant U.S. Department of the Treasury is an Executive Department of the United States of America and oversees the IRS and TIGTA.

19. Defendant Internal Revenue Service is a bureau of the U.S. Department of the Treasury and is responsible for the administration and enforcement of the Internal Revenue Code.

FACTUAL ALLEGATIONS

I. The IRS Willfully Failed To Establish Appropriate Administrative, Technical, And Physical Safeguards To Insure The Security And Confidentiality Of Mr. Griffin's Confidential Tax Return Information.

20. The IRS relies extensively on computerized systems of records to support its financial and mission-related operations. The IRS knows and has known that without effective security controls, the IRS's systems of records are vulnerable to, among other things, malicious efforts by IRS employees or contractors to illicitly obtain and misappropriate confidential taxpayer information.

21. As detailed above, however, TIGTA has put the IRS on notice for a decade that

²⁴ Defendants, as the United States, are proper party defendants in this action and have waived sovereign immunity pursuant to 26 U.S.C. § 7431 and 5 U.S.C. § 552a(g)(1)(D).

deficiencies in its “Security Over Taxpayer Data and Protection of IRS Resources” were the agency’s “number one major management and performance challenge area.”²⁵ Despite being aware of its security deficiencies for over a decade, the IRS willfully failed to establish appropriate administrative, technical, and physical safeguards to insure the security of confidential tax return information, including Mr. Griffin’s confidential tax return information.

22. For example, the IRS uses Microsoft Active Directory (“Microsoft AD”) services for its data security systems, including to facilitate secure user logon, access authorization, and credentialed validation for Windows laptops, desktops, and servers for all IRS employees, contractors, and business applications that interact with these computers.²⁶ The IRS is also supposed to use Microsoft AD to enforce the Internal Revenue Manual and operational standards for all Windows laptops, desktops, servers, user accounts, and service accounts.²⁷ In short, the IRS is supposed to use Microsoft AD to establish appropriate administrative, technical, and physical safeguards to protect Mr. Griffin’s confidential taxpayer information by, among other things, centralizing management of computers and users for data security purposes.²⁸

23. In September 2011, over a decade ago, TIGTA reported that “the IRS did not enforce the centralization of its Windows environment,” thus failing to establish safeguards to “achieve[] consistent identity and authentication management, [as] required by Federal regulations

²⁵ *SEE* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2021-20-001, ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE’S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2020, at 6 (October 2020).

²⁶ *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2018-20-034, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT AND CRIMINAL INVESTIGATION COMPUTER ROOMS LACK MINIMUM SECURITY CONTROLS, at 1 (June 2018).

²⁷ *Id.*

²⁸ *Id.*

and IRS enterprise architecture security principles.”²⁹ The IRS also “did not ensure that all Windows computers connected to its network were authorized and compliant with security policy, putting the IRS at risk of security breaches.”³⁰ And, although the IRS created standards to prevent unauthorized computers from being connected to the network, “it had not established a central controlling authority to enforce compliance with its policy.”³¹ In response, TIGTA recommended that the IRS establish a governing body that would, among other things, finalize and enforce security design criteria, develop standards, and ensure that unauthorized data systems are not implemented.³²

24. Seven years later, in 2018, after auditing the IRS’s implementation of TIGTA’s recommendation to establish certain technical and physical data security safeguards, TIGTA found, among other things, 88 physical security control weaknesses and over 1,700 improperly configured user accounts.³³ TIGTA also found that the IRS’s Windows Policy Checker was out of date and used three-year-old technical guidelines to conduct its analysis.³⁴ As a result, TIGTA concluded “the IRS cannot ensure that sensitive taxpayer information and taxpayer dollars are preserved and protected.”³⁵

25. The IRS continued its failure to implement appropriate safeguards through at least

²⁹ *Id.* (citing TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2011-20-111, CONTINUED CENTRALIZATION OF THE WINDOWS ENVIRONMENT WOULD IMPROVE ADMINISTRATION AND SECURITY EFFICIENCIES (Sept. 2011)).

³⁰ Report No. 2018-20-034 at 2.

³¹ *Id.*

³² *Id.*

³³ *Id.* at *Highlights*.

³⁴ *Id.*

³⁵ *Id.* at 5.

Fiscal Year 2020. For example, the Federal Information Security Modernization Act of 2014 (“FISMA”) required the IRS to establish appropriate administrative, technical, and physical safeguards over its system of records by, among other things, developing, documenting, and implementing an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. In its *Annual Assessment of the Internal Revenue Service’s Information Technology Program for Fiscal Year 2020*, however, TIGTA reported the following IRS failures, among others:

- **40% of the IRS’s Cybersecurity Framework Function Areas were deemed “Not effective.”**³⁶ Two out of five Cybersecurity Framework function areas (*i.e.*, Identify, Protect, Detect, Respond, and Recover) were deemed “not effective.”³⁷ Notably, *the IRS failed to effectively establish the organizational understanding to manage cybersecurity risks* to systems, assets, and capabilities (*i.e.*, the Identify function) and also failed to effectively establish and implement the appropriate activities to identify the occurrence of a cybersecurity event (*i.e.*, the Detect function).
- **Numerous Physical Security Violations in FY2020.**³⁸ The IRS is aware that physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. In Fiscal Year 2020, TIGTA performed site visits at six IRS locations to evaluate the physical security controls protecting the computer rooms housing the systems that collect, convert, and store a taxpayer’s confidential tax return information into electronic records of taxpayer data. Among other violations, TIGTA found six *violations of the Limited Access policies* in three of the six locations visited, where visitors and employees with access to larger processing areas also had “*uncontrolled access to the computer room*” that housed these data systems. Moreover, TIGTA also found “*multifactor authentication has not been implemented, as required*, for any of the Limited Area computer rooms in the six locations audited.”

³⁶ See Report No. 2021-20-001, at 7-9.

³⁷ *Id.* at 9.

³⁸ *Id.* at 13-14.

- **Access Management – 16,000 Account Policy Violations.**³⁹ Access management processes help to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. In Fiscal Year 2020, TIGTA performed two audits covering the IRS’s access management systems over 16,000 violations of the Internal Revenue Manual 10.8.1, *Information Technology (IT) Security – Policy and Guidance* requirements. Notably, TIGTA’s audit of controls to authenticate third-party authorization requests revealed that ***54% of the employees audited had unneeded access privileges to the IRS Centralized Authorization File***—*i.e.*, the computerized system of records which houses authorization information from both powers of attorney and tax information authorizations. Of the 54% of unauthorized users, 31% of them initiated actions to modify Centralized Authorization File authorizations between January 2, 2020 and February 29, 2020, despite these employees having jobs such as mail clerks, file supervisors, facility management, or computer assistant, none of which require them to change or add taxpayer authorizations to the Centralized Authorization File system.
- **Failure to Implement Encryption Algorithms.**⁴⁰ The IRS is supposed to use cryptography—*i.e.*, encryption algorithms that convert data into a format that is unreadable for unauthorized users—allowing confidential information to be transmitted or stored without unauthorized entities decoding it back into a readable format. In Fiscal Year 2020, the Government Accountability Office (“GAO”) performed an audit of the IRS’s information system security controls and found that the ***IRS failed to establish and implement cryptographic mechanisms to secure data in IRS systems*** that process taxpayer data. The GAO also found that the IRS failed to enforce the use of encryption algorithms as required by the Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules* for certain operating systems.

26. Similarly, TIGTA has found that the IRS failed to establish safeguards allowing the IRS to even *detect*, much less prevent, unauthorized access to confidential tax return information. Indeed, on July 31, 2020, TIGTA revealed that “the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and [Personally Identifiable Information].”⁴¹

³⁹ *Id.* at 21-22.

⁴⁰ *Id.* at 22.

⁴¹ See TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2020-20-033, MOST INTERNAL REVENUE SERVICE APPLICATIONS DO NOT HAVE SUFFICIENT AUDIT TRAILS TO DETECT UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION, at 2 (July 31, 2020).

In fact, 91% of monitored applications provided either “incomplete and inaccurate audit trails” or “no audit trails” at all.⁴² Likewise, on September 14, 2022, TIGTA reported that the IRS’s “current [physical security] processes do not ensure that recommended minimum security countermeasures are tracked and considered,”⁴³ particularly “because the IRS does not consistently use a centralized system to track physical security countermeasures, recommendations, approvals, implementation actions, and associated costs.”⁴⁴

27. Separately, the IRS is obligated to develop Plans of Action and Milestones (“POA&M”) for IRS systems to document its planned remediation actions to correct weaknesses. According to POA&M Standard Operating Procedures, “critical and high-risk vulnerabilities that cannot be remediated within 30 to 60 calendar days should be documented as POA&Ms in the Treasury Department’s FISMA Information Management System or the Authorizing Official should pursue a risk-based decision.”⁴⁵ TIGTA recently sampled 10 FISMA systems from the IRS’s database vulnerability scanning tool’s report that required POA&Ms, and on September 14, 2022, TIGTA reported that POA&Ms “were not created for database vulnerabilities” and “concluded that the IRS lacked managerial oversight to ensure that it appropriately documented corrective actions.”⁴⁶ As a result, “the IRS cannot ensure that it is correcting and managing its

⁴² *Id.* at *Highlights*, 2.

⁴³ TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-10-046, THE PROCESS FOR TRACKING PHYSICAL SECURITY WEAKNESSES IDENTIFIED IN IRS FACILITIES DOES NOT ENSURE THAT VULNERABILITIES ARE PROPERLY ADDRESSED, at 6 (September 14, 2022) (cleaned up).

⁴⁴ *Id.* at *Highlights*.

⁴⁵ TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, Report No. 2022-20-065, THE IRS NEEDS TO IMPROVE ITS DATABASE VULNERABILITY SCANNING AND PATCHING CONTROLS, at 9 (September 30, 2022).

⁴⁶ *Id.*

information security weaknesses [...] thereby exposing its systems to increased risk that nefarious actors will exploit the deficiencies to gain unauthorized access to information resources.”⁴⁷

28. The IRS’s failure to establish appropriate administrative, technical, and physical safeguards over its systems of records has been willful, at the very least, and upon information and belief, IRS personnel exploited these willful failures to misappropriate Mr. Griffin’s confidential tax return information and unlawfully disclose that information to ProPublica for further publication.

II. On Information And Belief, IRS Personnel Willfully Disclosed Mr. Griffin’s Tax Information, Including To ProPublica.

29. In response to a series of stories that ProPublica published in 2018 regarding how IRS budget cuts led to “an exodus of revenue agents, the kind of auditors [ProPublica claims] who really understand taxes and looked at corporations and the wealthy in particular,”⁴⁸ upon information and belief, IRS personnel exploited the IRS’s willful failures to establish adequate administrative, technical, and physical safeguards for the IRS’s data and records systems by misappropriating confidential tax return information for the highest U.S. taxpayers, including Mr. Griffin, for tax periods from at least 2013 and up to and including 2018. Specifically, continuing as late as 2019 (*i.e.*, when Mr. Griffin’s 2018 federal income tax returns would have been filed with the IRS), upon information and belief, IRS personnel misappropriated Mr. Griffin’s confidential tax return information for tax periods up to and including 2018 and then intentionally and maliciously disclosed those materials to ProPublica for further publication.

30. In or around March 2022, Mr. Griffin learned that ProPublica was in possession of

⁴⁷ *Id.*

⁴⁸ ProPublica, *The Inside Story of How We Reported the Secret IRS Files*, PROPUBLICA, August 6, 2021, <https://www.propublica.org/article/the-inside-story-of-how-we-reported-the-secret-irs-files>.

his confidential tax return information, along with the confidential tax return information “of thousands of the nation’s wealthiest people, covering more than 15 years.”⁴⁹ The information ProPublica obtained was “not just tax returns,” but also included “information that is sent to the IRS about financial activities” such as “income and taxes,” “investments, stock trades, gambling winnings and even the results of audits.”⁵⁰

31. Over the past year, ProPublica has steadily published more and more confidential tax return information of the taxpayers targeted by its articles, accompanied by what members of Congress describe as “politicized, misleading and likely inaccurate rhetoric and analysis.”⁵¹ For example, on April 13, 2022, ProPublica published confidential tax return information for Mr. Griffin’s 2013-2018 federal income tax years, including Mr. Griffin’s purported average annual income, purported percent of income deducted, and purported average effective federal income tax rate for those periods.⁵² In July 2022, ProPublica again published Mr. Griffin’s (and others’) confidential tax return information to criticize Mr. Griffin’s opposition to Illinois Governor J.B. Pritzker’s 2020 referendum to burden hard-working families in Illinois with yet more taxes.⁵³

⁴⁹ Jesse Eisinger, Jeff Ernsthausen & Paul Kiel, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, PROPUBLICA, June 8, 2021, <https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax>.

⁵⁰ *Id.*

⁵¹ Letter from Congressman Kevin Bradley and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf.

⁵² ProPublica, *America’s Top 15 Earners and What They Reveal About the U.S. Tax System*, PROPUBLICA, April 13, 2022, <https://www.propublica.org/article/americas-top-15-earners-and-what-they-reveal-about-the-us-tax-system>.

⁵³ Paul Kiel & Mick Dumke, *Ken Griffin Spent \$54 Million Fighting a Tax Increase for*

32. Defendants are well aware of the unlawful disclosures at issue in this lawsuit. Indeed, members of Congress have confirmed that there “is little doubt” that the confidential tax return information disclosed to ProPublica, including Mr. Griffin’s confidential tax return information, “came from inside the IRS [... and ...] does precisely what 26 U.S.C. § 6103 and related statutes were designed to prevent—the disclosure of private tax information and the political weaponization of that information.”⁵⁴

33. In July 2022, and again in August 2022, Mr. Griffin requested that Defendants “send a formal demand to ProPublica to return (and destroy any copies therewith) all of the confidential IRS data ProPublica has in its possession, custody, or control,” and further requested that Defendants provide Mr. Griffin information relevant to the IRS’s unlawful disclosure of his own confidential tax return information to ProPublica.

34. No Defendant has provided any meaningful response to Mr. Griffin’s requests.

COUNT I

Violation of 26 U.S.C. § 6103 – Willful or Grossly Negligent Unauthorized Disclosure

35. Mr. Griffin realleges and incorporates by reference paragraphs 1 to 34 as if fully set forth herein.

36. Title 26, U.S.C. § 6103 provides that tax “[r]eturns and return information shall be confidential” and prohibits disclosure and inspection by United States employees and other defined persons, except as specifically authorized in the provision.

37. Title 26, U.S.C. § 7431 provides taxpayers a private right of action for damages against the United States for the knowing or negligent unauthorized inspection or disclosure of tax

the Rich. Secret IRS Data Shows It Paid Off for Him, PROPUBLICA, July 7, 2022, <https://www.propublica.org/article/ken-griffin-illinois-graduated-income-tax>.

⁵⁴ Letter from Congressman Kevin Bradley and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury, dated April 18, 2022.

return information in violation of 26 U.S.C. § 6103.

38. “Return” is defined as “any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.”⁵⁵

39. “Return information” includes “a taxpayer’s identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense.”⁵⁶

40. “[D]isclosure” means “the making known to any person in any manner whatever a return or return information.”⁵⁷

41. As described above, on information and belief, IRS personnel—officers or employees of the United States—violated 26 U.S.C. § 6103 by disclosing Mr. Griffin’s confidential tax return information, for at least the tax periods from 2013-2018, to at least ProPublica, including Mr. Griffin’s wage information, charitable contributions, financial and

⁵⁵ 26 U.S.C. § 6103(b)(1).

⁵⁶ 26 U.S.C. § 6103(b)(2)(A).

⁵⁷ 26 U.S.C. § 6103(b)(8).

securities transactions, adjusted gross income, and information sufficient to calculate the purported effective federal income tax rates he paid for these years.

42. The IRS made these unlawful disclosures knowingly, or at the very least negligently or with gross negligence, including because the IRS willfully failed to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of Mr. Griffin's confidential taxpayer information from the unlawful disclosures alleged herein.

43. On information and belief, IRS personnel chose to disclose the confidential return information to ProPublica with the intent that ProPublica would widely publish the information through its website or through other means.

44. The IRS's disclosure of Mr. Griffin's tax return information did not result from a "good faith, but erroneous interpretation of section 6103,"⁵⁸ but rather from a knowing violation, gross negligence, or negligence.

45. The IRS's disclosure of Mr. Griffin's tax return information to ProPublica was not "requested by the taxpayer," Mr. Griffin, pursuant to 26 U.S.C. § 7431(b)(2).

46. The IRS's disclosure of Mr. Griffin's tax return information therefore violated 26 U.S.C. § 6103.

47. Pursuant to 26 U.S.C. § 7431, Mr. Griffin is entitled to statutory damages in the amount of \$1,000 per each act of unauthorized disclosure.

48. Mr. Griffin is also entitled to punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because the IRS's unlawful disclosure of his confidential tax return information was either willful or a result of gross negligence.

49. Mr. Griffin is entitled to the costs of the action and reasonable attorney's fees

⁵⁸ 26 U.S.C. § 7431(b)(1).

pursuant to 26 U.S.C. § 7431(c)(3) if he is the prevailing party in this action.

COUNT II
Violation of 5 U.S.C. § 552a(e)(10) – The Privacy Act

50. Mr. Griffin realleges and incorporates by reference paragraphs 1 to 34 as if fully set forth herein.

51. The IRS is an agency within the meaning of the Privacy Act.

52. The IRS maintained the records of Mr. Griffin, including his confidential tax return information, in a system of records as those terms are defined in the Privacy Act.

53. The IRS has long been aware of serious deficiencies in its safeguards, including as a result of repeated notice from TIGTA.

54. In violation of the Privacy Act, the IRS willfully and intentionally failed to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records, including Mr. Griffin's confidential tax return information, and failed to protect against any anticipated threats or hazards to those records' security or integrity, including those that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

55. The IRS also violated FISMA and provisions of the Internal Revenue Manual, as alleged herein, by failing to establish appropriate administrative, technical, and physical safeguards over its system of records.

56. As a direct and proximate result of its violations of the Privacy Act and FISMA, the IRS unlawfully disclosed, or failed to take reasonable steps to prevent its personnel from unlawfully disclosing, Mr. Griffin's records—his confidential tax return information—without his prior written consent and for no statutorily permitted purpose, in violation of 5 U.S.C. § 552a(b).

57. Mr. Griffin has and will continue to sustain damages directly traceable to the IRS's violations set forth above. Mr. Griffin is therefore entitled to damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kenneth C. Griffin respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

- A. Declaring that the IRS willfully, knowingly, and/or by gross negligence, unlawfully disclosed Mr. Griffin's confidential tax return information in violation of 26 U.S.C. § 6103;
- B. Declaring that the IRS willfully, knowingly, and/or by gross negligence, unlawfully inspected Mr. Griffin's confidential tax return information in violation of 26 U.S.C. § 6103;
- C. Awarding Mr. Griffin \$1,000 damages for each unauthorized disclosure of his tax return information, including subsequent disclosure, pursuant to 26 U.S.C. § 7431(c)(1) and damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4);
- D. Awarding Mr. Griffin reasonable costs and attorney's fees pursuant to 26 U.S.C. § 7431(c)(2)-(3) and as may otherwise be permitted by law;
- E. Ordering Defendants to produce to Mr. Griffin all documents in their possession, custody, or control regarding the inspection, transmittal, and/or disclosure of Mr. Griffin's confidential tax return information to ProPublica;
- F. Ordering the IRS to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act;
- G. Awarding pre-and post-judgment interest as allowed by law; and

H. Any such other relief as the Court deems just and proper.

JURY DEMAND

Pursuant to Rule 38(a) of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury of all claims asserted in this Complaint so triable.

Dated: December 13, 2022

Respectfully submitted,

By: /s/ Jason D. Sternberg

William A. Burck (*pro hac vice* forthcoming)

Derek L. Shaffer (*pro hac vice* forthcoming)

Alexander J. Merton (*pro hac vice* forthcoming)

QUINN EMANUEL URQUHART & SULLIVAN LLP

1300 I Street, N.W., Suite 900

Washington, DC 20005

(202) 538-8334

williamburck@quinnemanuel.com

derekshaffer@quinnemanuel.com

ajmerton@quinnemanuel.com

Christopher D. Kercher (*pro hac vice* forthcoming)

QUINN EMANUEL URQUHART & SULLIVAN LLP

51 Madison Avenue, 22nd Floor,

New York, New York 10010

(212) 849-7000

christopherkercher@quinnemanuel.com

John F. Bash, III (*pro hac vice* forthcoming)

QUINN EMANUEL URQUHART & SULLIVAN LLP

300 West 6th St, Suite 2010

Austin, TX 78701

(737) 667-6100

johnbash@quinnemanuel.com

Jason D. Sternberg (Florida Bar No. 72887)

QUINN EMANUEL URQUHART & SULLIVAN LLP

2601 South Bayshore Drive, Suite 1550

Miami, FL 33133

(786) 850-3607

jasonsternberg@quinnemanuel.com

Counsel to Plaintiff Kenneth C. Griffin