

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 10, 2025

The Honorable Andrew N. Ferguson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Chair Ferguson:

I write to request that the Federal Trade Commission (FTC) investigate and hold Microsoft responsible for its gross cybersecurity negligence, resulting in ransomware attacks against critical infrastructure, including U.S. health care organizations, which have caused enormous harm to health care providers, put patient care at risk, and continues to threaten U.S. national security.

Ransomware is a type of malicious software that cybercriminals use to extort victim organizations. Ransomware encrypts data and files on a computer or server, making them inaccessible. If the ransom is not paid, the entity's data remains unavailable. According to a report published in February 2025 by the Director of National Intelligence (DNI), there were over 5,000 ransomware attacks in 2024, a 15% increase over the prior year, and a 103% increase over 2022. According to the DNI, half of the targets of all ransomware attacks — worldwide — are against U.S. companies, government agencies and other organizations.

Microsoft makes Windows, the most widely used operating system for personal computers. In addition, Microsoft has a de facto monopoly over the operating systems used by most companies and government agencies. Microsoft chooses the default settings, including the security features that are enabled automatically and the required security settings (e.g. minimum password length). While organizations can change these settings, in practice, most do not.

In its default configuration, Microsoft Windows is incredibly vulnerable to ransomware infections. Because of dangerous software engineering decisions by Microsoft, which the company has largely hidden from its corporate and government customers, a single individual at a hospital or other organization clicking on the wrong link can quickly result in an organization-wide ransomware infection. Microsoft has utterly failed to stop or even slow down the scourge of ransomware enabled by its dangerous software. The FTC's mission to

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

protect Americans from deceptive and unfair business practices and promote fair competition obligates the agency to investigate Microsoft's negligence in a marketplace where its dominance has profound, foundational influence on cybersecurity practices and to hold the company accountable for its shortcomings.

My office has conducted oversight into the 2024 ransomware infection of Ascension, one of the largest non-profit health care systems in the U.S. This incident perfectly illustrates the problem caused by Microsoft. Ascension told my staff that in February 2024, a contractor using an Ascension laptop conducted a search using Microsoft's Bing search engine, which Microsoft's Edge web browser uses by default. The contractor clicked on a malicious link from one of the search results, which resulted in them inadvertently downloading and opening malware. After infecting that contractor's laptop, the hackers were able to move laterally within Ascension's network and gain administrative privileges to accounts on the organization's Microsoft Active Directory server, which is one of the crown jewels of an organization's network because it is used to manage user accounts. The hackers were able to use this privileged access to push ransomware to thousands of other computers in the organization, which created challenges to Ascension's ability to serve its patients and communities. The hackers were also able to use this privileged access to steal sensitive data of 5.6 million patients.

The hackers exploited a technique called Kerberoasting to gain access to privileged accounts on Ascension's Microsoft Active Directory server. This hacking technique leverages Microsoft's continued support by default for an insecure encryption technology from the 1980s called RC4 that federal agencies and cybersecurity experts, including experts working for Microsoft, have for more than a decade warned is dangerous. Although Microsoft's software also supports a secure encryption technology approved and recommended by the U.S. government, known as the Advanced Encryption Standard, this vastly superior encryption technology is not required by default in Windows. Microsoft's continued support for the ancient, insecure RC4 encryption technology needlessly exposes its customers to ransomware and other cyber threats by enabling hackers that have gained access to any computer on a corporate network to crack the passwords of privileged accounts used by administrators. According to Microsoft, this threat can be mitigated by setting long passwords that are at least 14 characters long, but Microsoft's software does not require such a password length for privileged accounts.

My staff spoke with senior Microsoft officials on July 29, 2024 and urged the company to warn its customers of the serious threat posed by the Kerberoasting hacking technique and the fact that Microsoft's software is vulnerable in its default configuration. On October 11, 2024, Microsoft acted on this request. The company published a blog post that recommended actions that organizations can adopt to protect against this hacking technique and announced that the company is working on a software update that will disable the dangerous RC4

encryption technology. Eleven months later, Microsoft has yet to release that promised security update.

While my staff specifically requested that Microsoft publish and publicize clear guidance in plain English so that senior executives would understand this serious, avoidable cyber risk, Microsoft instead published a highly technical blog post on an obscure area of the company's website on a Friday afternoon. Microsoft took no meaningful steps to publicize this blog post. Moreover, Microsoft declined to explicitly warn its customers that they are vulnerable to the Kerberoasting hacking technique unless they change the default settings chosen by Microsoft. As such, it is highly likely that most companies, government agencies, and nonprofits that are Microsoft customers remain vulnerable to Kerberoasting.

Although Microsoft is clearly not treating Kerberoasting as a serious threat, U.S. and allied cybersecurity agencies are. The Cybersecurity and Infrastructure Security Agency (CISA) issued public guidance for the health care sector on December 15, 2023 which included warnings about Kerberoasting and the need to disable RC4 encryption. CISA, the Federal Bureau of Investigation, and the National Security Agency (NSA), along with several foreign partner agencies, issued joint guidance on October 16, 2024 focused on mitigating Iranian cyber threats, which specifically warned about Kerberoasting and the importance of disabling RC4. Finally, CISA and NSA co-issued a comprehensive, 68-page guide authored by Australia's national security agencies in September 2024, focused specifically on defending against hacks targeting Microsoft's Active Directory software. The first threat described in that guide is Kerberoasting.

To be clear, Kerberoasting is just one technique used by hackers to exploit vulnerabilities in Microsoft software, and the Ascension hack is just one example. For example, in July 2023, I asked the FTC, CISA and the Department of Justice to hold Microsoft responsible for another cybersecurity lapse that enabled a major hack of U.S. government agencies by China. A subsequent review of that incident by the Cyber Safety Review Board, which I requested, assessed that "Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations." Just this July, yet another Microsoft cybersecurity lapse reportedly enabled Chinese government-linked hackers to exploit a vulnerability in Microsoft's SharePoint software to steal sensitive documents from U.S. government agencies and corporate customers. But the Ascension hack illustrates how it is Microsoft's customers, and, ultimately, the public, who bear the cost of Microsoft's dangerous software engineering practices and the company's refusal to inform its customers about the pressing need to adopt important cybersecurity safeguards.

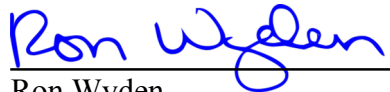
There is one company benefiting from this status quo: Microsoft itself. Instead of delivering secure software to its customers, Microsoft has built a multibillion dollar secondary business

selling cybersecurity add-on services to those organizations that can afford it. At this point, Microsoft has become like an arsonist selling firefighting services to their victims. And yet government agencies, companies, and nonprofits like Ascension have no choice but to continue to use the company's software, even after they are hacked, because of Microsoft's near-monopoly over enterprise IT.

I urge the FTC to investigate Microsoft and hold the company responsible for the serious harm it has caused by delivering dangerous, insecure software to the U.S. government and to critical infrastructure entities, such as those in the U.S. health care sector. Without timely action, Microsoft's culture of negligent cybersecurity, combined with its de facto monopolization of the enterprise operating system market, poses a serious national security threat and makes additional hacks inevitable.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator
Ranking Member, Committee
on Finance