Executive Summary

The purpose of this report is to provide a high-level overview of the state's outstanding debt as of September 30, 2024. Per West Virginia Code, the West Virginia State Treasurer's Office (WVSTO) prepares quarterly debt update reports. The March and September reports are shorter-in-length, three-month updates. The June and December reports are more detailed, covering six months of the fiscal year. In addition, the WVSTO compiles an Annual Debt Report as of June, summarizing the entire fiscal year.

This report is the first for fiscal year 2025. Tax supported debt as of September 30, 2024, decreased approximately $28.6 million from the June 30, 2024 balance. Non tax-supported debt increased $331.6 million during the same time period.

The month of October is designated as National Cybersecurity Awareness Month. Cybercriminals appear to be capitalizing on a recent IT outage that affected an estimated 8.5 million electronic devices in mid-July. The incident started with a faulty software update from CrowdStrike and triggered massive IT outages across the global economy.

Federal government officials and cybersecurity experts warn that in the aftermath, malicious phishing websites were created to appeal to people looking for information on the attack. These phony websites instead harvest people's personal information.

As state agencies and spending units increasingly rely on electronic forms of communication for daily operations and financial transactions, awareness of phishing attacks is essential to preventing cyber-attacks and data breaches.

Phishing attempts are growing in prominence every day and have the potential to cripple a state agency or spending unit by initiating a data breach.

What is Phishing?

Phishing is a form of cyber fraud in which an attacker masquerades as a reputable entity or person using a channel of electronic communication, such as text message, email, or voicemail. Email is the most common communication channel used in phishing attempts since it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than breaking through a computer's defenses using direct computer hacking. In initiating a phishing attempt using email, the attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials, account information, or personally identifiable information (PII) from victims.

Types of Phishing Attacks

Spear Phishing: Spear phishing occurs when a phishing attack is customized to target an organization or specific individuals. These attacks involve gathering additional information ahead of time and incorporating other elements, such as logos, email and website addresses of the organization or other businesses the organization works with, and sometimes professional or personal details of a target, in order to appear as authentic as possible. This additional effort by the attacker tends to pay off with a larger number of targets being duped.

Whale Phishing (Whaling): As a variation of the spear phishing attack, whaling targets an organization's senior executives. Whaling attacks typically take specific responsibilities of these executive roles into consideration, using focused messaging to trick the victim. When a whaling attack successfully dupes a target, the attacker's windfall can be substantial (e.g. high-level credentials to an organization's passwords and accounts).

Clone Phishing: Another variation on spear phishing attacks is clone phishing. In this attack, targets are presented with a copy (or "clone") of a legitimate message they had received earlier, but with specific changes the attacker has made in an attempt to ensnare the target (e.g., malicious attachments, invalid URL links, etc.). Because this attack is based on a previously viewed legitimate message, it can be effective in duping a target.

Voice Phishing (Vishing): Vishing is a phishing attack conducted via telephone. The purpose of the telephone call is to obtain information, such as bank account or credit card numbers. These attacks often use a fake Caller ID profile to impersonate a legitimate business, governmental agency, or charitable organization.

SMS Phishing (Smishing): Smishing is a phishing attach conducted through SMS messages. Smishing attacks usually lure the user into visiting a site that entices them to download malicious apps or content.

How to Protect Against Phishing Attacks

Pay attention to the sender's email address. If the sender's email address looks suspicious, don't open the email. Sometimes the "from" address in a phishing message will appear to be perfectly valid but will have a different address from the organizations name.

Be cautious about opening attachments or clicking on links in emails. Even your work colleagues' accounts could be hacked. If the attachment or link provided in an email looks weird, don't click it. Files and links can contain malware that can weaken your computer's security.

Do your own typing. If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself. Even though a link or phone number in an email may look like the real deal, scammers can hide the true destination.

Make the call if you're not sure. Do not respond to any emails that request personal or financial information that are outside of your ordinary course of business. Phishers use pressure tactics and prey on fear. If you think a company, or other vendor really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.

Use multi-factor authentication (MFA). Even if a phishing target's credentials have been compromised in a phishing attack, MFA requires a second level of verification, such as an access code sent to your phone, before gaining access to a sensitive account.

While it is impossible to prevent phishing attacks by cyber criminals, awareness of basic phishing techniques is crucial in preventing potential cyber-attacks and data breaches.

Article Works Cited: *"What Is a Phishing and How Does It Work? | Synopsys."* *www.synopsys.com, www.synopsys.com/glossary/what-is-phishing.html#:~:text=In%20a%20phishing%20attack%2C%20bait.*

Federal Trade Commission. "How to Recognize and Avoid Phishing Scams." Consumer Information, Sept. 2022, www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

If you have comments or questions, please feel free to let me know.

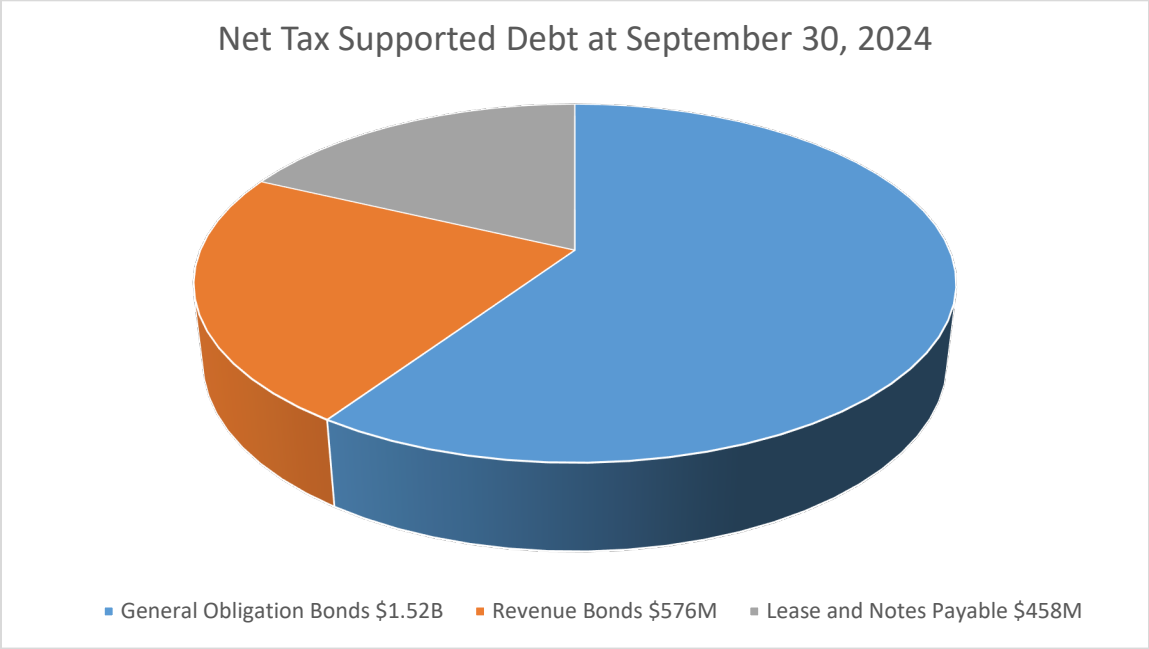
Contact Information:
Joellen Lucas, Director of Debt & Securities Management
315 70th Street SE, Charleston, WV 25304
304-340-1572 or joellen.lucas@wvsto.gov
Website: Debt Management

Debt Position Report

Update: September 30, 2024

One of the most important measurements of debt for a state, city, county or any other municipal bond issuer is the amount of net tax-supported debt outstanding. The State of West Virginia had a net tax-supported debt of $2.55 billion as of September 30, 2024.

The net tax-supported debt calculation does not include claims and judgments, accrued compensated absences, pension costs, other post-employment benefits costs or other liabilities of the state. Those obligations are detailed in the state's Annual Comprehensive Financial Report (ACFR) available from the Division of Finance of the Department of Administration or online at www.wvfinance.state.wv.us.



DISCLAIMER

Pursuant to W.Va. Code §12-6A-6, every state spending unit is required to report quarterly on its debt to the West Virginia State Treasurer's Office. The Treasurer's Office prepares this Report using information provided by the spending units and information from other sources considered reliable. This report is unaudited and may be amended when updated information is provided to the Treasurer's Office.

Spending units not reporting debt updates for first quarter: Parkways Authority, WV Board of Licensed Dieticians, Division of Forestry, Department of Health, Health Facilities and Human Services, Public Employees Grievance Board, WV Division of Rehabilitation, and the Secretary of State.

West Virginia Net Tax-Supported Debt Outstanding as of September 30, 2024

Type of Debt		Principal Outstanding September 30, 2024
GENERAL OBLIGATION BONDS		
Safe Road Bonds	$ 22,090,000	
Roads to Prosperity Bonds	1,450,755,000	
Infrastructure Improvement Bonds	42,812,275	
Total General Obligation Bonds		$ 1,515,657,275
REVENUE BONDS		
Economic Development Authority, Lottery Revenue Bonds	251,680,000	
Economic Development Authority, Excess Lottery Revenue Bonds	89,110,000	
Higher Education Policy Commission, Lottery and Excess Lottery Revenue Bonds	216,767,500	
Higher Education Policy Commission, Excess Lottery Revenue Bonds (BABs)	50,265,000	
School Building Authority, Lottery Revenue Bonds	74,468,858	
School Building Authority, Excess Lottery Revenue Bonds	72,455,000	
School Building Authority, Excess Lottery Revenue Bonds (QSCBs)	150,480,000	
West Virginia Infrastructure & Jobs Development Council (Excess Lottery Revenue Bond)	46,305,000	
Total Revenue Bonds		951,531,358
TOTAL LEASE OBLIGATIONS / NOTES PAYABLE		458,392,334
GROSS TAX SUPPORTED DEBT		2,925,580,967
DEDUCTIONS FOR ESCROW/SINKING FUND/RESERVE FUNDS		
Economic Development Authority, Excess Lottery Revenue Bonds	(28,747,412)	
Economic Development Authority, Lottery Revenue Bonds	(135,940,000)	
Higher Education Policy Commission Excess Lottery Revenue Bonds	(79,220,000)	
School Building Authority, Excess Lottery Revenue Bonds	(17,350,000)	
School Building Authority, Excess Lottery Revenue Bonds (QSCBs)	(114,600,642)	
Total Deductions		(375,858,054)
NET TAX-SUPPORTED DEBT		$ 2,549,722,913

Debt Position Report

Update: September 30, 2024

The State of West Virginia has more than 20 bonding authorities that may issue revenue bonds backed by various pledges of revenue. Each authority has its own specific parameters such as volume caps, interest rate caps, etc., which is codified in relevant sections of the West Virginia Code. The authorities listed below have outstanding debt that is self-supporting and is not considered as part of the state's direct debt burden. This debt is considered non tax-supported debt.

West Virginia Non Tax-Supported Debt Outstanding as of September 30, 2024

Issuer	Principal Outstanding September 30, 2024
Commissioner of Highways	160,860,000
Concord University	13,396,233
Economic Development Authority	5,527,601,589
Fairmont State University	45,799,447
Glenville State University	34,260,299
Higher Education Policy Commission	26,183,780
Hospital Finance Authority	3,520,812,352
Housing Development Fund	719,935,000
Marshall University	93,510,000
Parkways Authority	465,490,000
Shepherd University	27,181,702
Tobacco Settlement Finance Authority	613,804,000
Water Development Authority	115,003,000
West Liberty University	13,277,832
West Virginia Infrastructure & Jobs Development Council	76,080,000
West Virginia State University	34,713,046
West Virginia University	727,908,869
NON TAX-SUPPORTED DEBT (net)	$12,215,817,149