

TIM SCOTT, SOUTH CAROLINA, CHAIRMAN
ELIZABETH WARREN, MASSACHUSETTS, RANKING MEMBER

MIKE CRAPO, IDAHO
MIKE ROUNDS, SOUTH DAKOTA
THOM TILLIS, NORTH CAROLINA
JOHN KENNEDY, LOUISIANA
BILL HAGERTY, TENNESSEE
CYNTHIA LUMMIS, WYOMING
KATIE BOYD BRITT, ALABAMA
PETE RICKETTS, NEBRASKA
JIM BANKS, INDIANA
KEVIN CRAMER, NORTH DAKOTA
BERNIE MORENO, OHIO
DAVID MCCORMICK, PENNSYLVANIA

JACK REED, RHODE ISLAND
MARK R. WARNER, VIRGINIA
CHRIS VAN HOLLEN, MARYLAND
CATHERINE CORTEZ MASTO, NEVADA
TINA SMITH, MINNESOTA
RAPHAEL G. WARNOCK, GEORGIA
ANDY KIM, NEW JERSEY
RUBEN GALLEGO, ARIZONA
LISA BLUNT ROCHSTER, DELAWARE
ANGELA D. ALSOBROOKS, MARYLAND

CATHERINE FUCHS, STAFF DIRECTOR
JON DONENBERG, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON BANKING, HOUSING, AND
URBAN AFFAIRS

WASHINGTON, DC 20510-6075

December 15, 2025

The Honorable Scott Bessent
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Ave, NW
Washington, D.C. 20220

The Honorable Pamela Bondi
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

Dear Secretary Bessent and Attorney General Bondi:

I write to request information about whether the Department of the Treasury and the Department of Justice are investigating significant national security risks posed by decentralized cryptocurrency exchanges like PancakeSwap. PancakeSwap has reportedly been used to help launder the cybercrime proceeds and huge sums of money for North Korea.¹ I am especially concerned about any improper political influence by the Trump Administration on enforcement decisions, because PancakeSwap has reportedly been “drumming up interest among traders to use coins issued by the Trump family’s main crypto company, World Liberty Financial.”² The *Wall Street Journal* reports that “[o]ver 90% of [World Liberty’s flagship coin] USD1 trades have taken place on PancakeSwap,” which would make it USD1’s primary trading platform.³ As Congress considers crypto market structure legislation—including rules to prevent terrorists, criminals, and rogue states from exploiting decentralized finance (DeFi) to fund their activities—it is critical to understand whether you are seriously investigating these risks.

PancakeSwap is a decentralized cryptocurrency exchange that advertises itself as a place where users can “[i]nstantly swap crypto tokens [with] no registration or account needed.”⁴ PancakeSwap’s financial transactions are carried out automatically by computer programs known as “smart contracts.”⁵ As the Treasury Department has warned, these automatic processes have created a dangerous misperception that

¹ Allium, “Bybit Hack: How the Lazarus Group Exploited DeFi Protocols to Launder \$400M,” Marcus Chua and Carlos Cortés-Gómez, March 26, 2025, <https://www.allium.so/post/bybit-hack-how-the-lazarus-group-exploited-defi-protocols-to-launder-400m>.

² Wall Street Journal, “The Recipe Behind the Trump Family’s Crypto Riches: PancakeSwap,” Angus Berwick and Patricia Kowsmann, August 12, 2025, <https://www.wsj.com/finance/currencies/trump-family-crypto-1e7ab14a>.

³ *Id.*

⁴ PancakeSwap, “Product Overview,” <https://docs.pancakeswap.finance/>.

⁵ PancakeSwap, GeneralGeeneral FAQ,” <https://docs.pancakeswap.finance/welcome-to-pancakeswap/contact-us/faq>.

decentralized services can ignore anti-money laundering safeguards, even though they function like other financial institutions.⁶ Exchange platforms like PancakeSwap and Uniswap facilitate hundreds of millions of dollars in transactions per day⁷ and do not require users to register or show any form of identification to trade.⁸ These lax requirements permit users to bypass the “know your customer” (KYC) rules that other types of financial institutions are required to follow.⁹ This seems to be by design because PancakeSwap describes this loophole in its token offerings, “[a]nyone...can take part — [with] no KYC required.”¹⁰

Without anti-money laundering program controls, including but not limited to KYC, bad actors are able to exploit decentralized platforms to move, mix, and cash out illicit funds. For example, North Korean hackers used PancakeSwap to facilitate the laundering of an estimated \$263 million of the \$1.46 billion they stole in what has been described as the “largest crypto theft of all time.”¹¹ Experts familiar with the incident have explained how “[North Korea’s] laundering process...relied heavily on decentralized finance (DeFi) tools, particularly decentralized exchanges (DEXs) and cross-chain bridges.”¹² Treasury has also previously recognized that North Korea’s “significant state-sponsored hacking and money laundering campaign...funds Pyongyang’s weapons of mass destruction and missile program.”¹³

Decentralized exchanges like PancakeSwap have been described as the “Perfect Off Ramp for Criminals,” given that they can enable criminals to “convert ill-gotten gains into cash that can be spent in the real world...with minimal verification and KYC controls.”¹⁴ Bad actors anonymously convince unsuspecting victims into giving them crypto, swap it for other coins, and then walk away with money that is much harder for law enforcement to trace. In one scheme, scammers did exactly that: they used PancakeSwap to defraud victims, and then sent funds to notorious mixers like TornadoCash to further obfuscate the money trail.¹⁵ Recent research finds that these kinds of investment schemes are extremely common, with over “384,000 scammer addresses...on Uniswap...and Pancakeswap.”¹⁶

Without regulatory monitoring, illicit actors will increasingly be able to acquire crypto assets on decentralized exchanges, and then facilitate financial transactions without having to cash out through

⁶ U.S. Department of the Treasury, “Illicit Finance Risk Assessment of Decentralized Finance,” April 2023, p. 2, <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>.

⁷ CoinMarketCap, “Uniswap vs PancakeSwap,” Werner Vermaak, <https://coinmarketcap.com/academy/article/uniswap-vs-pancakeswap>.

⁸ New York Post, “Inside the No-KYC crypto craze shaking up Wall Street,” Ariel Zilber, September 25, 2025, <https://nypost.com/business/best-no-kyc-crypto-exchanges>.

⁹ WIRED, “New Clues Suggest Stolen FTX Funds Went to Russia-Linked Money Launderers,” Andy Greenberg, October 12, 2023, <https://www.wired.com/story/ftx-hack-400-million-crypto-laundering>.

¹⁰ PancakeSwap, “CAKE.PAD,” <https://pancakeswap.finance/kepad>.

¹¹ Allium, “Bybit Hack: How the Lazarus Group Exploited DeFi Protocols to Launder \$400M,” Marcus Chua and Carlos Cortés-Gómez, March 26, 2025, <https://www.allium.so/post/bybit-hack-how-the-lazarus-group-exploited-defi-protocols-to-launder-400m>; CoinDesk, “North Korean Hackers Were Behind Crypto’s Largest ‘Theft of All Time,’” Aoyon Ashraf, February 21, 2025, <https://www.coindesk.com/markets/2025/02/21/north-korean-hackers-were-behind-crypto-s-largest-left-of-all-time>.

¹² TRM Labs, “Bybit Hack Update: North Korea Moves to Next Stage of Laundering,” March 3, 2025, <https://www.trmlabs.com/resources/blog/bybit-hack-update-north-korea-moves-to-next-stage-of-laundering>.

¹³ Letter from Jonathan Blum, Principal Deputy Assistant Secretary, Office of Legislative Affairs, Department of Treasury, to Senators Reed and Warren, June 12, 2025, https://www.banking.senate.gov/imo/media/doc/20250612_response_to_20250519lettertodojtreasuryrenorthkoreacryptoheist.pdf.

¹⁴ TRM Labs, “On the Trail of the Squid Game Scammers,” January 11, 2023, <https://www.trmlabs.com/resources/blog/on-the-trail-of-the-squid-game-scammers>.

¹⁵ *Id.*

¹⁶ “Serial Scammers and Attack of the Clones: How Scammers Coordinate Multiple Rug Pulls on Decentralized Exchanges,” Phuong Duy Huynh et al., February 2025, <https://dl.acm.org/doi/10.1145/3696410.3714919>.

institutions that could otherwise have monitored and reported suspicious activity to law enforcement. Industry reports and regulators have sounded the alarm: Chainalysis's 2025 Crypto Crime Report found that illicit activity has become "increasingly diverse and professionalized" and that "malicious actors often launder stolen funds by funneling them through decentralized exchanges (DEXs), mining services, or mixing services to obfuscate the transaction trail and complicate tracing."¹⁷ Elliptic noted that "[i]n 2018, money laundering using cryptoassets...occurred almost entirely using Bitcoin" but "[t]oday, illicit activity in cryptoassets involves sophisticated actors" who use "stablecoins and services in the decentralized finance (DeFi) ecosystem."¹⁸ In 2023, Treasury warned that "DeFi services at present often do not implement AML/CFT controls or other processes to identify customers," and that "[a] lack of AML/CFT controls [is] one of the primary goals of decentralization."¹⁹

You and your departments have significant responsibilities for safeguarding the American people and the U.S. financial system. The public deserves to know whether you are investigating the serious risks identified by national security experts and the crypto industry itself. To help me fulfill my legislative responsibilities, I ask that you provide answers to the following questions no later than January 12, 2025:

1. Describe any and all potential national security risks associated with decentralized exchanges, including exchanges like PancakeSwap.
2. Describe the gaps in current statutory and regulatory authorities that could be closed to address national security risks associated with decentralized exchanges.
3. List any and all specific actions the agency will take to prevent conflicts of interest and insulate national security and law enforcement decisions from crypto-related conflicts of interests, including business ties to the Trump family.

Sincerely,



Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs

¹⁷ Chainalysis, "The 2025 Crypto Crime Report," February 2025, pp. 2 and 76,

<https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf>.

¹⁸ Elliptic, "Elliptic's Typologies Report: Innovating to fight financial crime in an age of rapid change," October 1, 2025, <https://www.elliptic.co/blog/elliptics-typologies-report-innovating-to-fight-financial-crime-in-an-age-of-rapid-change>.

¹⁹ U.S. Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," April 2023, p. 26, <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>.