NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

# Attending the Draft in Green Bay? Protect Against Identity Theft

**FOR IMMEDIATE RELEASE:** April 3, 2025
**Contact:** Caleb Kulich, Public Information Officer, (608) 621-1290
caleb.kulich@wisconsin.gov

MADISON, Wis. – With hundreds of thousands of visitors expected to attend the upcoming Draft in Green Bay, it is possible that those attending the event and spending time in the surrounding areas will be targeted by identity thieves hoping to steal private information. Any travel, but especially travel to popular locations and events, can increase the risk of identity theft. Consumers should be aware of how identity theft occurs, and how to reduce their risks, in preparation for the weekend.

Before and during the Draft, scammers will likely use many methods to convince consumers to give up personal information. Surveys, prize giveaways, and online quizzes not affiliated with official Draft events can be tempting. However, if they require participants to provide private data, even as simple as their name, birth date, or contact information, consumers should remember they have no control over what happens to that data after it is submitted. Many of these innocent-seeming collection methods are actually run by individuals and groups for the sole purpose of selling the personal information.

Websites and apps often solicit personal information, and request device access and permissions that many consumers do not question. Bad actors may also create websites and apps with misleading names or branding to imply they are affiliated with the 2025 Draft. Consumers should always refer to official event sources and retailers when registering or making purchases related to the Draft.

When traveling to and from the Draft, the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) recommends that consumers make purchases with a credit card because they offer built-in protections against fraud, allow the user to dispute fraudulent charges, and can be quickly cancelled if lost or compromised.

DATCP also encourages card users to be vigilant, as the data on a card can be stolen in several ways. Aside from physical theft, scammers can place 'card skimmer' devices on a legitimate business payment processor device without the knowledge of the business. These devices record card data while it is being used to make a purchase. Card skimmers have been found on ATMs, gas station card readers, and even retail business checkouts. Often, a small camera or fake keypad is installed to record the card's PIN.

To protect against card skimmers, consumers should perform a brief inspection of the card reader device before they use their card. Beware if the card reader is misaligned or sticking out at a strange angle, the keypad feels flimsy or appears to be separating from the device, or if physically wiggling the card reader dislodges a card skimmer device or component. Devices sometimes called card "shimmers" function similarly but capture data from tap-to-pay transactions. Suspected card skimmers and shimmers should be reported to the business.

Many providers now build safety measures into their cards to prevent this form of theft. Consumers concerned about the vulnerabilities of an older credit card may consider requesting a new card from their provider with newer data security protections before traveling.

For more information and identity theft resources or for assistance with identity theft recovery, visit DATCP's Consumer Protection webpage at ConsumerProtection.wi.gov or contact the Consumer Protection Hotline at (800) 422-7128 or DATCPHotline@wisconsin.gov.

###

*Find more DATCP news in our newsroom, on Facebook, X, and Instagram.*