

# Even NPIs Are Subject to Identity Theft

**Thousands**  
of NPIs are stolen  
each year.<sup>1</sup>

National Provider Identifiers (NPI) are a primary part of the identity of health care professionals like you and are susceptible to potential cyberattacks and identity theft.

## The Vulnerability of NPIs

Why are these identifiers so vulnerable to theft? For starters, they are publicly available through the National Plan and Provider Enumeration System. But they're also easily obtainable by anyone with access to electronic medical records.

## Stay Ahead of NPI Fraud with NPI Alerts

With thousands of NPIs stolen each year<sup>1</sup>, it's important that they be closely monitored. ID Watchdog<sup>®</sup> can help. Through our NPI Alerts feature, we monitor the NPI Database for changes associated with your NPI number and alert you if your account has been modified in a way that, if unrecognized, could indicate identity theft.

We monitor the NPI Database for potentially fraudulent activity to help you better defend yourself against NPI fraud.

## What Could Happen When an NPI is Stolen

- 1** Fraudsters use the NPI to submit fraudulent health care claims or prescription fill requests in the corresponding provider's name.
- 2** Fraudsters then receive payment for treatment that was never provided or prescriptions that were not prescribed.
- 3** When the insurance company and IRS become privy to the fraudulent claims, **the provider could be held responsible for reimbursement of payments made—and the taxes.**<sup>2</sup>

## Keep Informed. Become Less Vulnerable.

Activating the NPI Alerts feature is easy—simply opt-in, **enter your provider ID and stay up-to-date on activity related to your NPI.**

To learn more about ID Watchdog and how we can help you better protect your identity, **visit [idwatchdog.com](https://www.idwatchdog.com)**

(1) "Prevent theft of your National Provider Identifier" Physicians Practice (2) "Your NPI Is Easy to Steal; Here's How to Prevent That" Medscape