

## Trade Secrets and the IKR

How does one prove the existence of a Trade Secret without exposing the secret?

Exposing the Trade Secret to “too” many people or to people under the wrong conditions may forfeit ones potential legal protection.

Yet, unlike Copyrights, Patents, and Trademarks, no economy has implemented a central Trade Secret registry because, among other issues:

- A central repository is a potential target for thieves, hackers, etc.; and/or
- The process of registering a Trade Secret could potentially expose the secret itself or subject it to potential risk of theft (e.g. when the Trade Secret is sent to the registry).

Furthermore, in this age of digital creation and communications, Trade Secrets are typically stored as digital files which could be easily stolen and disseminated, as electronic files are so easily spread online and over the internet. Furthermore, theft via the electronic copying of a million page document and/or a complex CAD file is as easy as the stealing a single page.

So what is the solution? The IKR from IIPCC.

As soon as one create a “new” Trade Secret and save it digitally (e.g., as a .docx, .mp4 file, .mpg file, .pdf file, .jpg file, Google Doc, etc.) the IKR will quickly and easily provide an irrefutable time/date stamp and digital signature to prove the creation of ones “new” Trade Secret. The date/time stamp provides an important temporal record while the signature uniquely identifies the digital file without exposing the content in any way.

The IKR record is then stored with WIPO and or trusted international organization(s).

The IKR offers key advantages:

1. Evidence of creation, stored with world-recognized bodies, that can be used to help resolve future / potential disputes (i.e. to convincingly demonstrate that you created the Trade Secret before anyone else);
2. No exposure of the Trade Secret itself (the digital signature can later be used to authenticate, but not recreate, the digital file); and/or

3. A standardized time stamp<sup>1</sup>, produced using internationally recognized time sources, provides consistency, thus eliminating inconsistency issues caused by potentially-conflicting metadata (e.g. different digital creation dates and times) that may, in turn, be caused by:
  - a. Improperly-maintained personal or business systems (servers, desktop computers, tablets, mobile phones, etc.) producing inaccurate times and dates;
  - b. Inaccurate time clocks on individual systems; and/or
  - c. Inconsistencies among different systems.

---

<sup>1</sup> The IKR determines the time based on Network Time Protocol (NTP). Each IIPCC IKR server synchronizes with its local pool.ntp.org. In addition, the US IIPCC IKR server will use the time.nist.gov server.