

Data Manipulation: Get the Facts

What is data manipulation?

Today, more than 92 percent of critical business records are generated, managed and stored electronically, creating efficiencies and cost-savings for businesses. Unfortunately, digital information can be easily deleted, altered and/or manipulated. For businesses, the burden of proof is on the company to ensure and attest to the accuracy and credibility of their electronic business records. This ability to prove the integrity of critical business records becomes especially important in litigation where executives are often called upon to support their claims of ownership of any discoverable records, as well as verify their history of creation and use.

What are some examples of data manipulation?

Electronic records have been proven to have been manipulated in cases ranging from stock options fraud to loan fraud to intellectual property disputes.

Some recent examples of actual cases surrounding the manipulation of electronic records include:

- Top executives at a successful technology company attempted to alter electronic records to hide a secret options-related slush fund to cover the tracks of their backdating options scheme.
- A prominent real estate developer received an electronic version of a loan agreement to print and sign. Rather than just signing the document, he made subtle changes to it in order to make the terms of the loan more favorable to himself. The changes went undetected for a year until the loan was refinanced.
- An auditor impeded a federal investigation by intentionally altering, destroying and falsifying the financial records of a now defunct credit card issuer in order to downplay or eliminate evidence that there were "red flags" that he should have caught.
- Two major Wall Street firms settled with the SEC after being accused of "late trading." Late trading or "after-hours" trading involves placing orders for mutual fund shares after the market close, but still getting that day's earlier price, rather than the next day's closing price.
- A prominent scientist, funded by millions of dollars in state and private funding was charged with fraud and embezzlement, after admitting that he manipulated photo images of stem cells in his research.

How can data manipulation be prevented?

Eliminating the risk that critical business records can be deleted, altered or manipulated in any way is best accomplished through a combination of sound business practices and supporting data-level technology. For instance, a solid first line of defense is to ensure that only authorized individuals have access to critical business records.

In addition to strong corporate policies governing the access and usage of stored digital information, there are a number of data-level integrity solutions available to organizations today. The most effective of these solutions provide objective, non-collusive proof of business record integrity that is independent of an organization's people, processes and technology, as well as a method to validate record integrity over the long-term, regardless of changes in an organization's technology infrastructure. Trusted time stamping is a good example of a solution that meets these criteria.

What is trusted time stamping and how does it work?

Trusted time stamping provides organizations with the ability to establish when a document was created and that it was never altered. When it is integrated into a records management process, trusted time stamps can be used to soundly verify the content and time integrity of the electronic document and prove that it has never been tampered with over the course of its useful life. In addition, trusted time stamps never expire, so they can be used to prove the integrity of documented created decades ago, even if a company's hardware, software or technology providers change.

A trusted time stamp is created when a time stamping authority (TSA) acts as a trusted third-party issuer of time-stamp tokens that associate a time and date with a digital document in a cryptographically secure way. The time stamp is digitally stored with the original data.

Are there standards to ensure the validity of trusted time stamping?

There are two leading international standards governing the use of trusted timestamp technology: the American National Standard X9.95-2005 Trusted Time Stamp Management and Security Standard (ANSI X9.95) and ISO/IEC 18014.

ANSI X9.95 is the first American National Standard for data-level controls and specifies the minimum security requirements for the effective use of trusted time stamps in a financial services environment. There are several advantages to the X9.95 standard. First, this standard provides flexibility by offering five different accepted time-stamping methods, allowing end users to choose the method that best fits their needs. Second, ANSI has developed audit control objectives and recommends best practices for business, operational and technical use against which a time stamp vendor may be evaluated or audited. Thus, end users are guaranteed a higher level of assurance. Finally, this standard is vendor-neutral, so end users are not limited to a specific vendor or technology in order to utilize trusted time-stamping technologies.

ISO/IEC 18014 is a three-part international standard that defines a general model for time-stamping services along with specific service instances. The standard defines a total of 5 different time-stamping services, enabling end users to choose the method that best fits their needs. Since the standard precisely defines the data structures and protocols used to interact with each type of time-stamping service, it provides the basis for interoperability between time-stamping vendors. The

benefit to end users is wider integration of time-stamping capabilities into vendor products, portability of timestamps between vendor products, and greater flexibility in choosing and migrating between vendor products.

Is trusted time stamping admissible in a court of law?

When companies enter into legal challenges, all relevant documentation, both electronic and paper, is discoverable and admissible in the eyes of the court. Trusted time stamping can be used to prove the integrity of an electronic record in a legal proceeding. This is beneficial not only for proving that data manipulation has or has not occurred, but also for verifying intellectual property claims. For instance, by applying a trusted time stamp to research and development records, a company can prove they are the original creator of an asset, and prove the history of its creation and use.