# Electronic Data Authenticity and Integrity As a Service

*Proving and Legally Defending the Authenticity of Data Managed in the Cloud*

**Tom Klaff, CEO**

*October 28, 2009*

# Agenda

- **Definitions:** What is Data Integrity and Authenticity?
- **Real Life Examples:** Why Data Integrity is an Issue
- **Impact:** What are the Operational Threats and Legal Risks?
- **The Chain-of-Custody Problem:** Proving Data Integrity and Authenticity in the Cloud
- **Solution:** Electronic Data Integrity & Authenticity as-a-service
- **Success:** A Case Study
- **Key Conclusions**

# Tamper Detection is Part of Our Physical World

*But what about our "digital world" ?*

# Data Integrity vs. Data Authenticity

## RECORD MANAGEMENT PHASE

### DATA INTEGRITY:

Assurance that data has not been altered (intentionally or unintentionally) in the normal course of business operations between “here" and “there," or between "then" and "now.”

## DISCOVERY PHASE

### DATA AUTHENTICITY:

Assurance to any ***legal or regulatory entity*** that data has not been altered (intentionally or unintentionally) in the normal course of business operations between “here" and “there," or between "then" and "now.”

**LITIGATION HOLD**

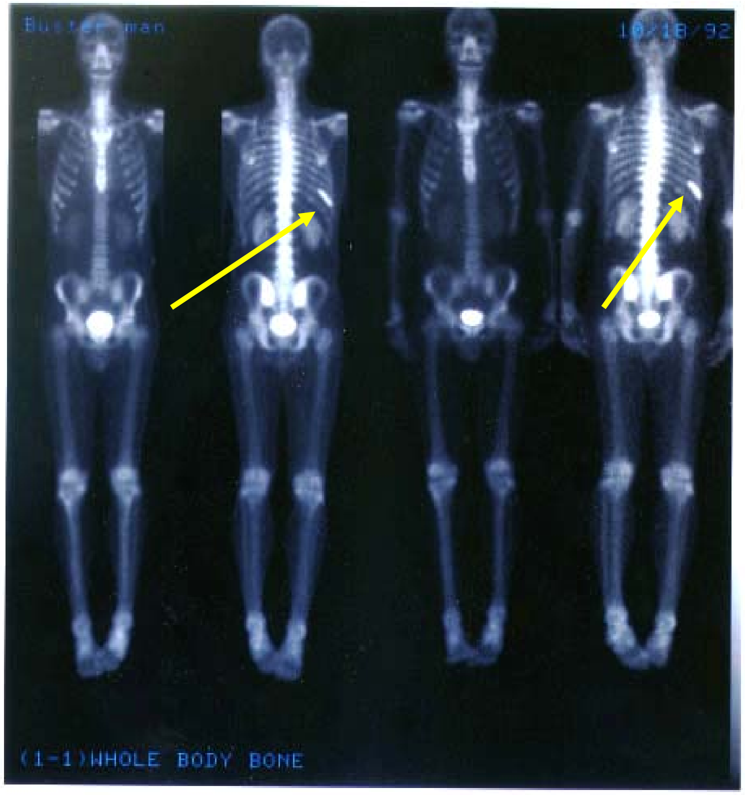
**(T = 20 years)**

**(T = 150 - 300 days)**

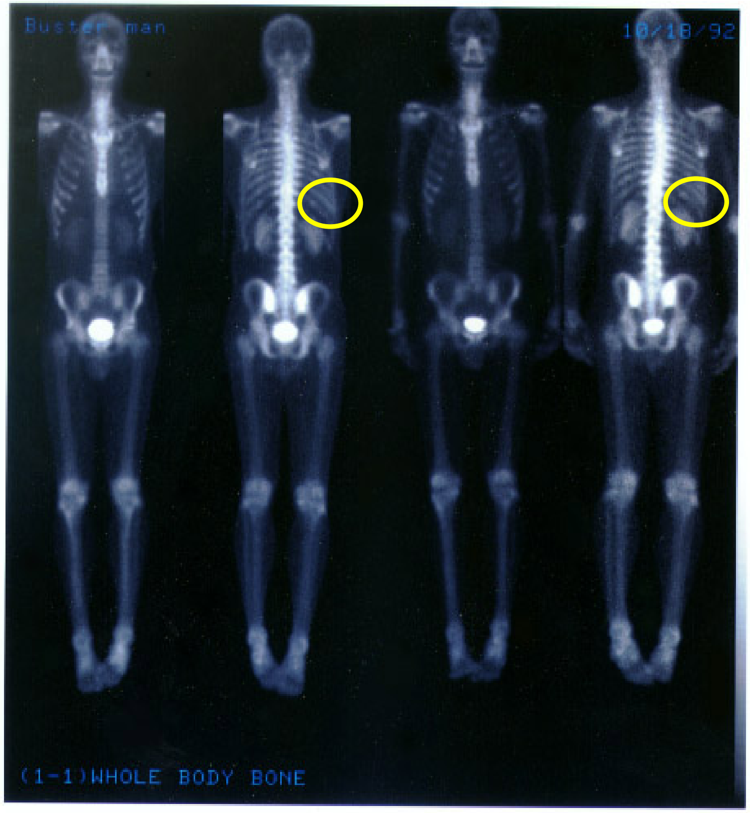
# Tamper Detection is Extremely Difficult

# Electronic Record Tampering

*Easy to do…hard to authenticate*



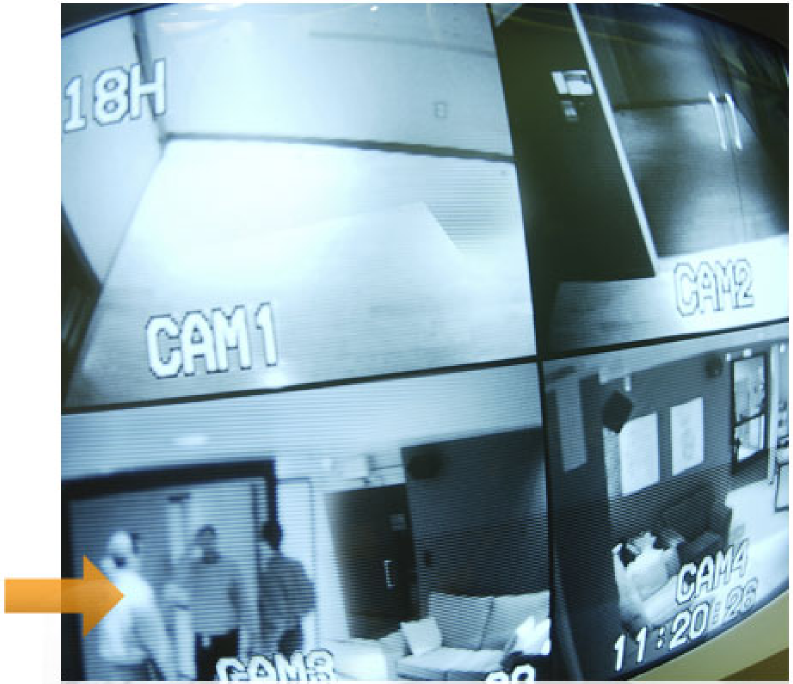
**Patient with cancerous lesions on rib in 2nd and 4th images…**



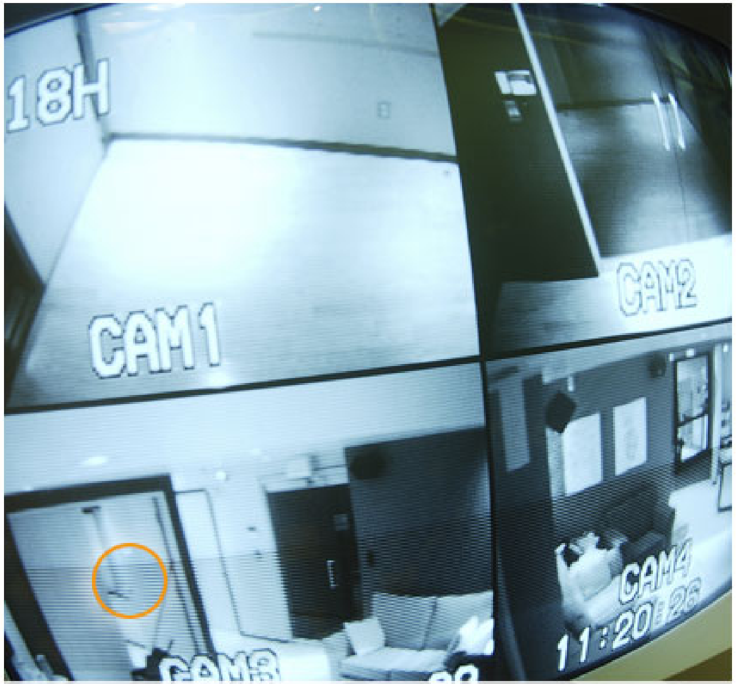
**…Same patient, miraculously cured…. courtesy of Adobe Photoshop**

# Altering Electronic Video Surveillance

## *Covering tracks*



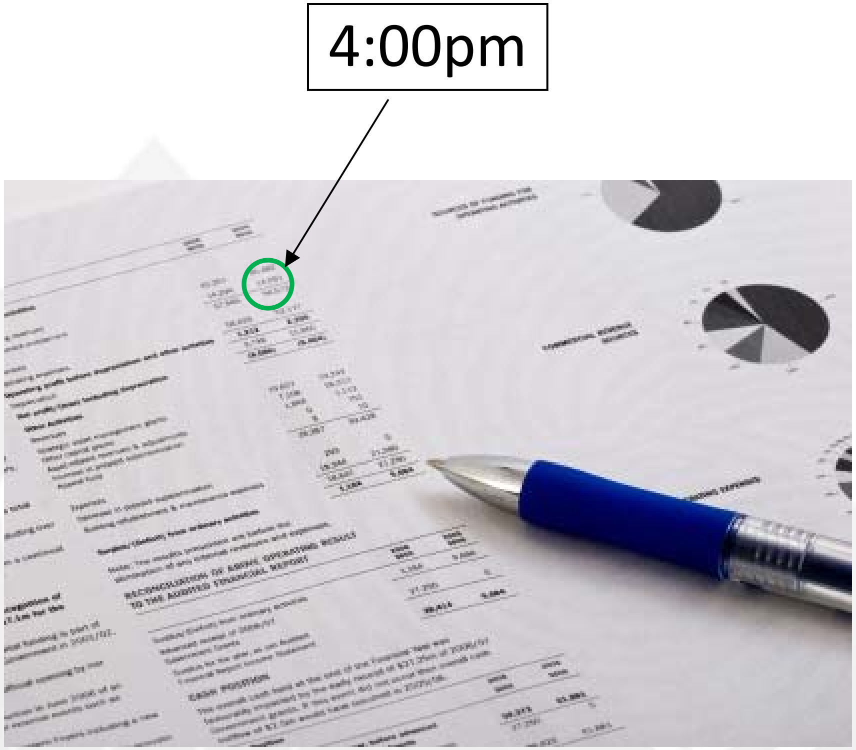
**There are three men in this building at 11:20:26 …**



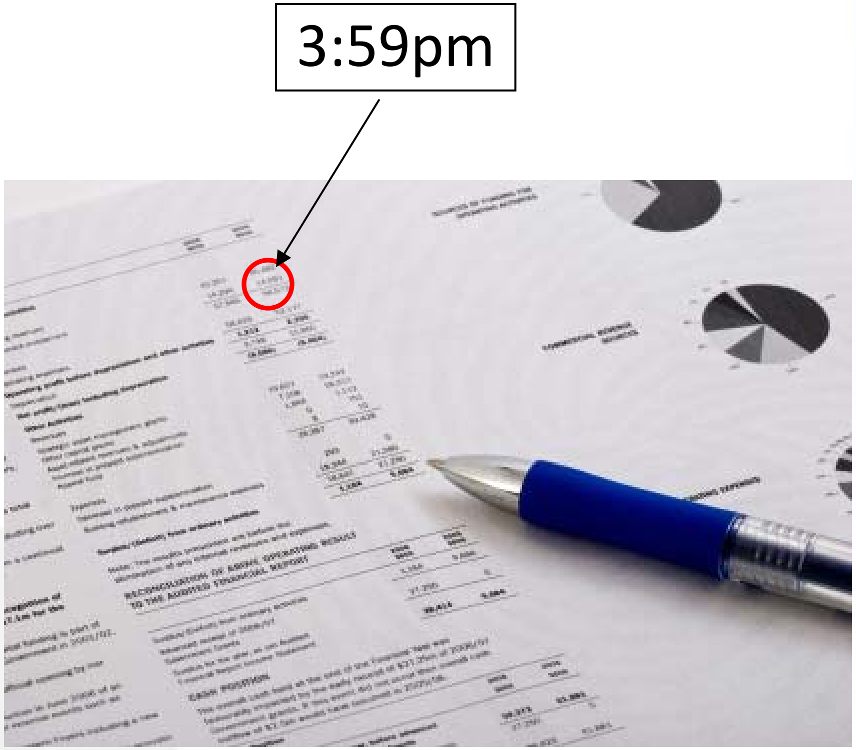
**… what happened to them?**

# Late Trading

*Stealing wealth*



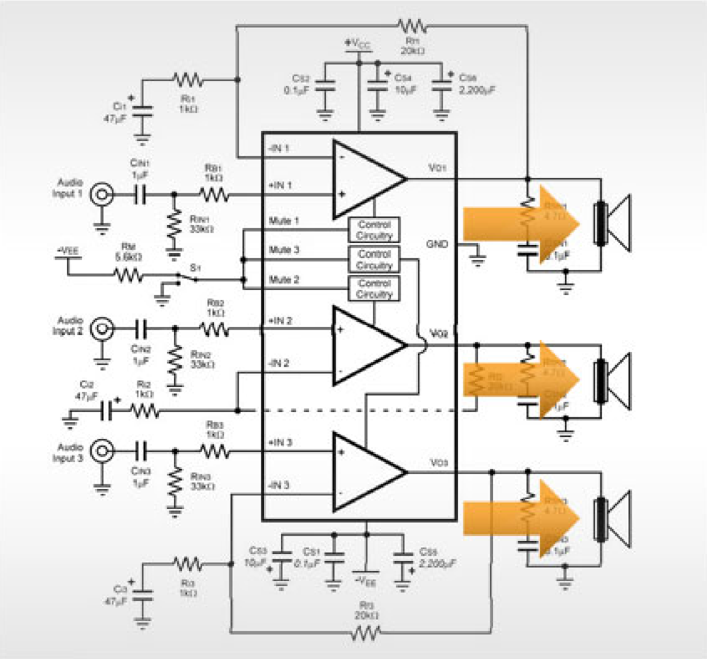
4:00pm

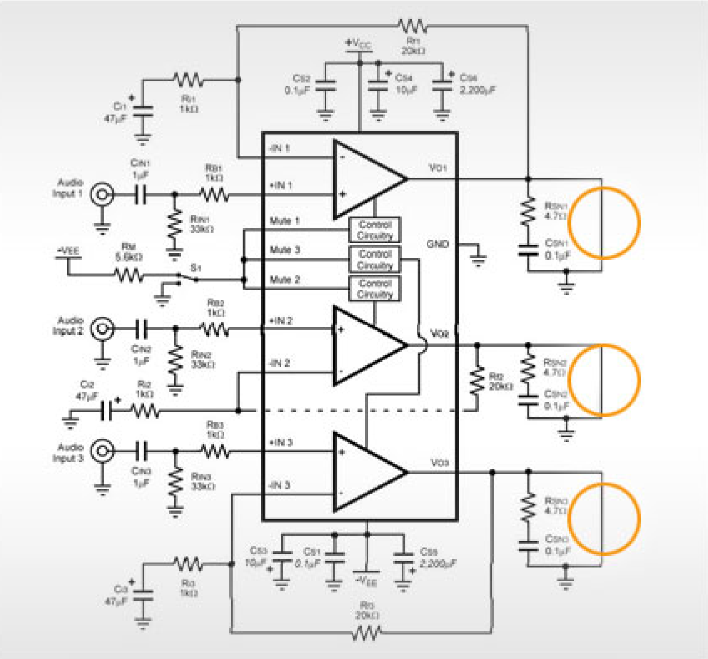


3:59pm

# Stealing Intellectual Property Content

## *Ensuring a head-start at whatever cost*





**This schematic found its way into the hands of a competitor, courtesy of a departed engineer …**

**… what was left behind in the organization's archive by the recently departed engineer**

# Proving Data Authenticity

## *Why it is important*

- **Intellectual Property Protection**
  - Prove ownership of trade secrets and ideas
  - Mitigate risks when developing new content or collaborating
- **Motivated Insider**
  - “Covering tracks”
  - Protecting reputations
  - Concealing problems
- **Information Lifecycle Risk**
  - System upgrades
  - Employee turnover
  - Chain-of-custody
- **Proving You Have Good Operating Practices**
  - Needed step in records management workflow
- **Lawyers and Regulators Understand Data Authenticity Issues**
  - Amended Federal Rules of Civil Procedure

# Data Authenticity: A Vital Legal Defense

**"When the facts are weak, attack the process that manages the facts."**

-- *Tim Carroll, Esq., Vedder Price*

Ask the questions - "Is it ***possible*** that…

…data changed throughout its chain-of-custody?"

…Joe, an administrator, could have manipulated your files and audit logs?"

…outside parties gained unauthorized administrative access to your service?"

…metadata were changed during systems upgrades or data transmission?"

…data changed during the systems migration after the merger last month?"

…the EHR system you manage has been breached and the records changed?"

…your surveillance evidence has been tampered during its chain-of-custody?"

# Rulings from the Bench

## *Requirements of authenticity*

“. . . The record being proffered ***must be shown to continue to be an accurate representation*** of the record that originally was created.”

– Judge Klein, *American Express Travel Related Services Co., Inc. v. Vee Vinhnee*

“[T]he inability to get evidence admitted because of a ***failure to authenticate*** it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation.”

– United States Magistrate Judge Paul Grimm, *Lorraine v. Markel*

“First, judges may well begin demanding authentication foundations that do more than constitute trivial showings….Unless you know how to ***oppose the authentication foundation*** of your opponent, you will miss out on this ***opportunity to exclude evidence*** from being admitted.”

– George Paul, Esq., *Foundations of Digital Evidence*

“If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent ***to plan to authenticate the record by the most rigorous standard*** that may be applied.”

– Judge Paul Grimm, *Lorraine v. Markel*

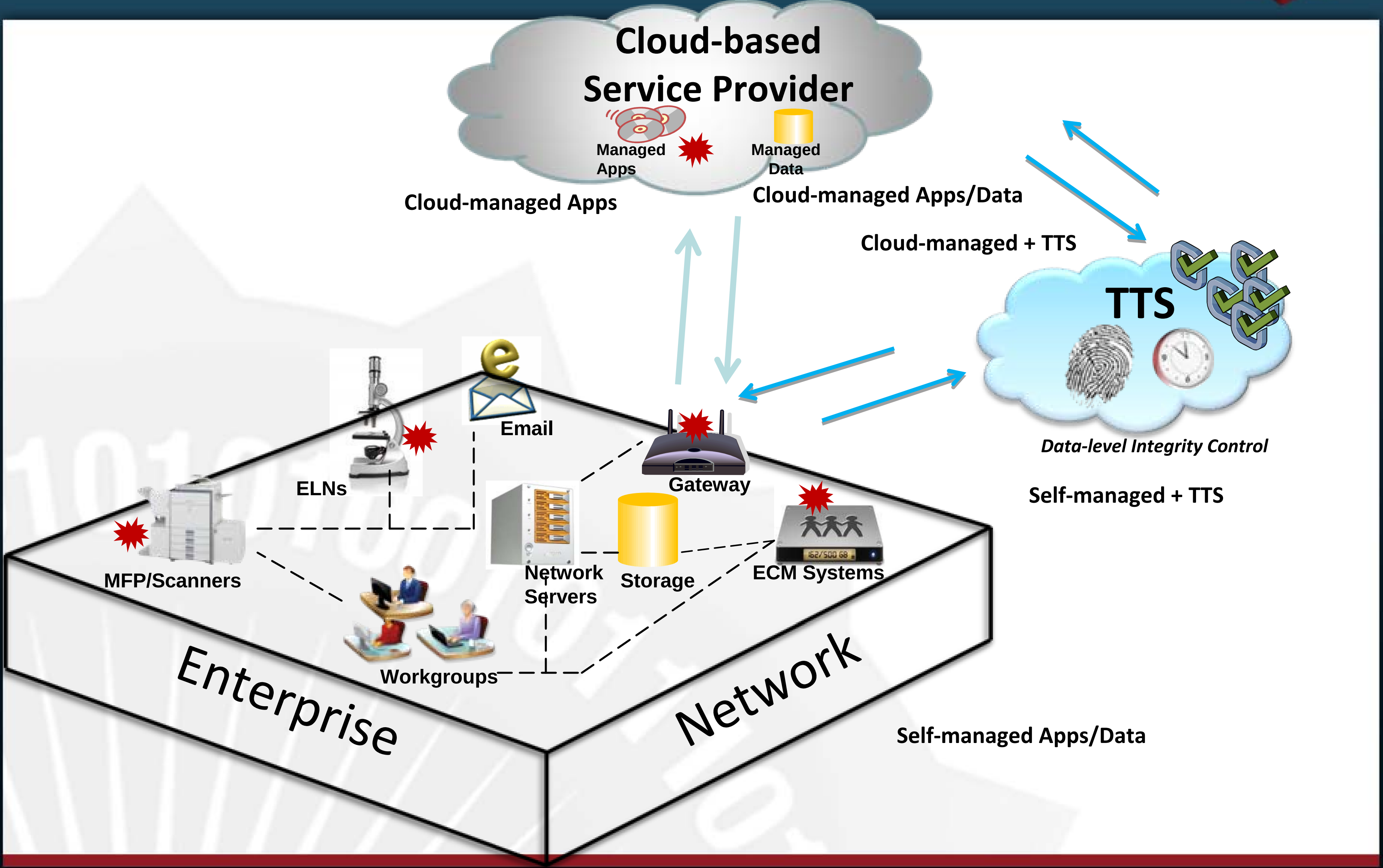
# The Chain-of-Custody Threat is Real

## *Relevant case law*

- **Chain-of-Custody**
  - the unbroken trail of accountability that ensures and proves the physical security of samples, data, and records
- **Case Law Examples:**
  - *Coca-Cola v. Pepsi (2006)*
  - *Best Buy v. Microsoft (2007)*
  - *South Korea Health Ministry v. Hwang Woo-suk (2005)*
  - *U.S. Government v. Daniel Calugar, Security Brokerage Inc. (2005)*
  - *Aguilar v. Benner Convalescent Center (2005)*

# Chain-of-Custody in the Cloud

## *How authenticity as-a-service mitigates data integrity risk*



# Comparative Benefit Analysis

## *Impact on Data Integrity*

| KEY VARIABLES | Self-managed Apps/Data | Cloud-managed Apps | Cloud-managed Apps/Data | Clouds-managed Apps/Data + TTS | Self-managed Apps/Data + TTS |
|---|---|---|---|---|---|
| COST | 🔴 | 🟢 | 🟢 | 🟢 | 🔴 |
| CONTROL | 🟢 | 🟡 | 🔴 | 🔴 | 🟢 |
| RISK | 🟡 | 🔴 | 🔴 | 🟢 | 🟢 |
| TRANSPARENCY | 🟡 | 🟡 | 🔴 | 🟢 | 🟢 |
| LEGALLY DEFENSIBLE | 🔴 | 🔴 | 🔴 | 🟢 | 🟢 |

| | |
|---|---|
| Worst | 🟥 |
| Medium | 🟨 |
| Best | 🟩 |

# Managing Electronic Trade Secrets

*Corporate & strategic risk case study*

## Global Semi-conductor Company Case Study

The Case:

- Scientist joined competitor
- New product launched
- Injunction filed
- 2 + years in Discovery
- 7 years of paper notebooks
- Sales Impact: “Wait & See”
- Sales Impact II: Indemnity
- Lost case: No Proof

| BUSINESS RISK | BUSINESS IMPACT |
|---|---:|
| **Revenue from Patent** | $200,000,000 |
| **Costs:** | |
| Legal Fees | $2,000,000 |
| Opportunity Cost | $3,000,000 |
| Revenue Lost (Neg. Pub.) | $10,000,000 |
| Lost Royalties (Lost Patent) | $59,550,000 |
| **Total Risk** | **$274,550,000** |

***Solution:* *Migrated to ERM processes with integrated, automated integrity protection and authentication controls***

# How Legally Defensible is your Data?

*Delivering assurance and peace-of-mind*

## Can your TTS guarantee its time stamps and process will withstand the toughest legal scrutiny?

- **Can't Be Forged**
  - Would require breaking two widely analyzed hash algorithms
- **Independently Provable**
  - Time and content integrity can be independently validated
  - Proof doesn't depend on process or proprietary technology
- **Protection Lasts the Lifetime of the Record**
  - No keys or certificates to expire
  - Not subject to key compromise or digital signature limitations
- **Protection Cannot Be Invalidated**
  - Not subject to key compromise
- **Legally Defensible**
  - Will withstand the toughest legal scrutiny
- **Backed by a Leading Litigation Support Firm**
  - A Sworn Affidavit – signed testament by an expert attesting to the defensibility of the time-stamp service
  - Access to an Independent Expert Witness bench
  - Expert Witness Testimony
  - Money-back Guarantee

# That’s Where We Come In

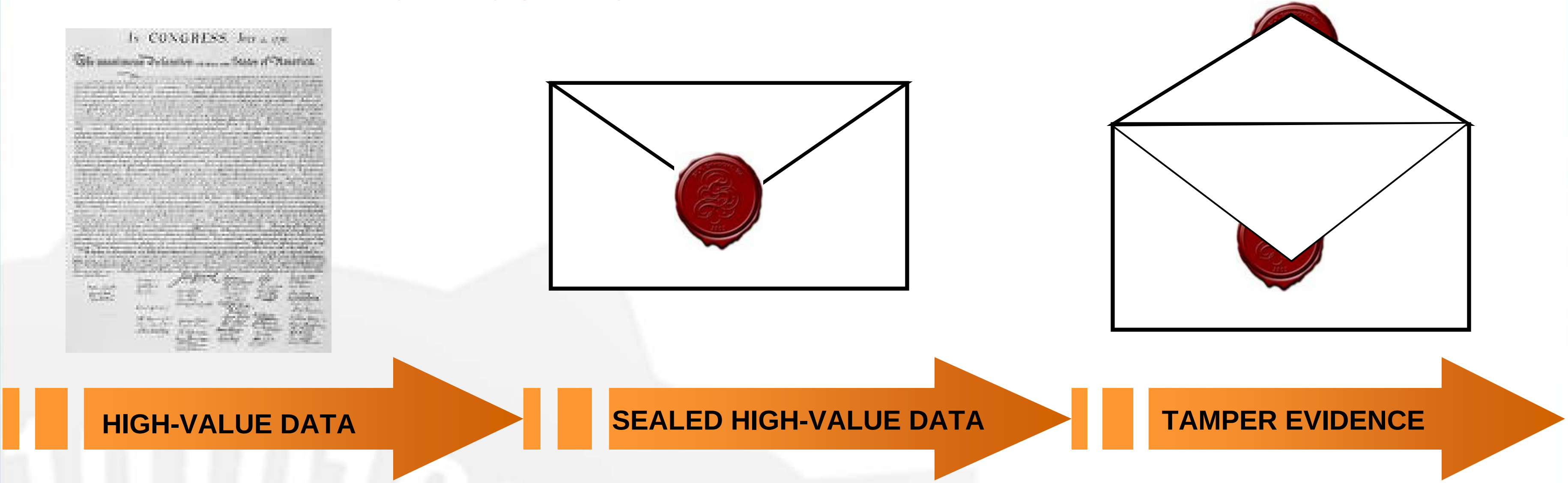
## *Surety overview*

- **Who we are…**
  - Headquartered in Reston, VA
  - International footprint - Surety Korea
  - Founded in 1994, by prominent Bellcore scientists who pioneered the concept of trusted, digital timestamping (cryptographically based)
- **Problem we solve…**
  - Protect the integrity and prove the authenticity of electronic records, files and other digital content (intellectual property content, legal evidence content)
- **Why is this a problem?**
  - “Bet-the-business issue” in litigation, regulatory compliance and IP defense
- **Technology expertise**
  - Trusted time-stamp technology; patented approach (hash-chain linking)
- **Core service offering**
  - AbsoluteProof® Trusted Time-Stamp Service (ANSI X9.95 and ISO/IEC-18014-3 compliant)
- **Legally defensible - Guaranteed**
  - Technology and process will withstand the toughest legal scrutiny – we guarantee it

# Nothing New

## *Same need...new medium*

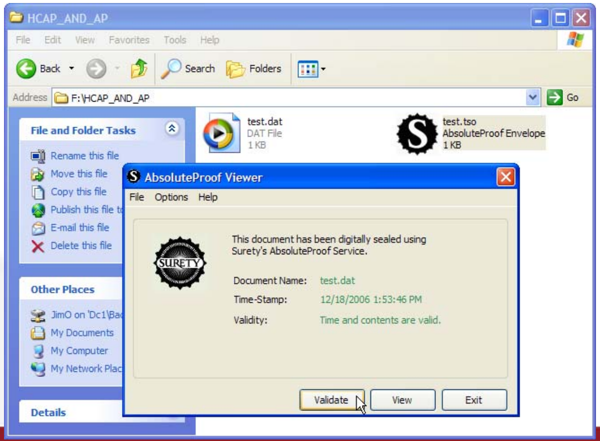
## That Was Then....


HIGH-VALUE DATA

SEALED HIGH-VALUE DATA

TAMPER EVIDENCE

## This is Now....



Address: F:\HCAP_AND_AP

test.dat
DAT File
1 KB

test.tso
AbsoluteProof Envelope
1 KB

This document has been digitally sealed using Surety's AbsoluteProof Service.

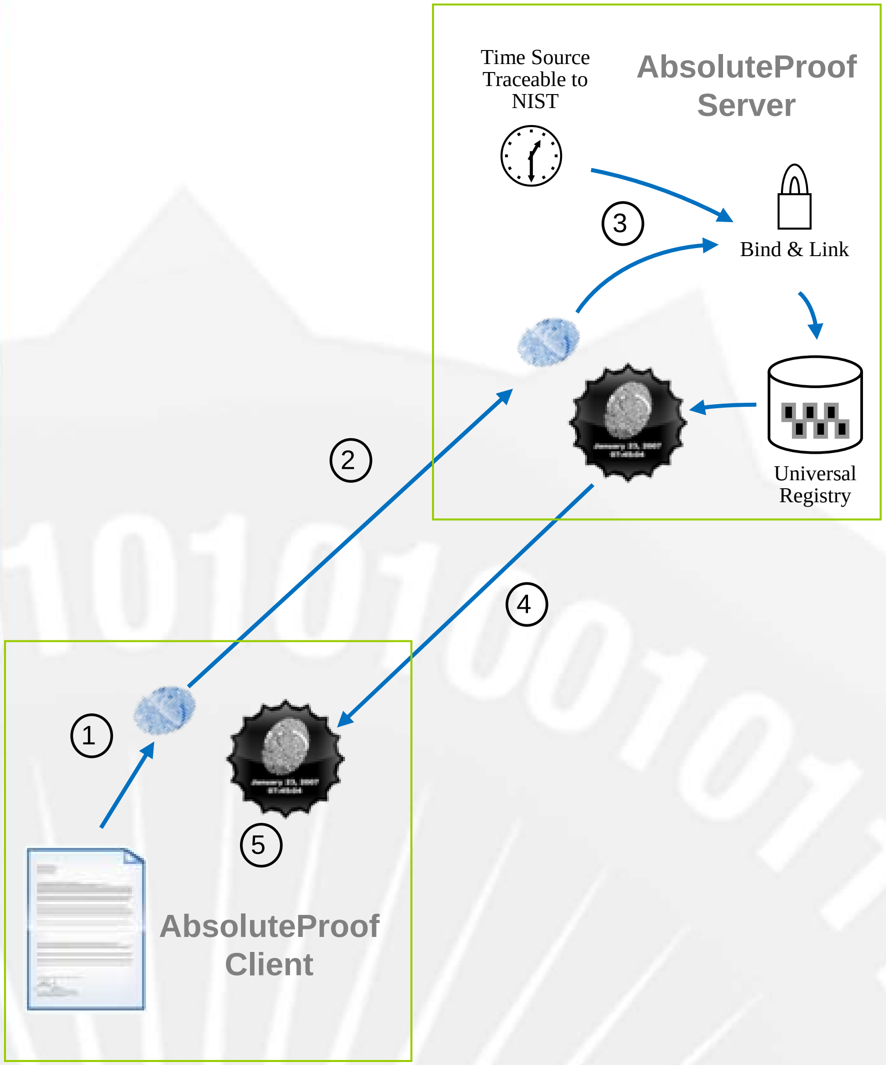
Document Name: test.dat

Time-Stamp: 12/18/2006 1:53:46 PM

Validity: Time and contents are valid.

# AbsoluteProof Service – How We Do It

*Record sealing process*



1. AbsoluteProof Client creates a hash of an electronic file

2. AbsoluteProof Client sends hash to AbsoluteProof Server, via secure Internet Connection

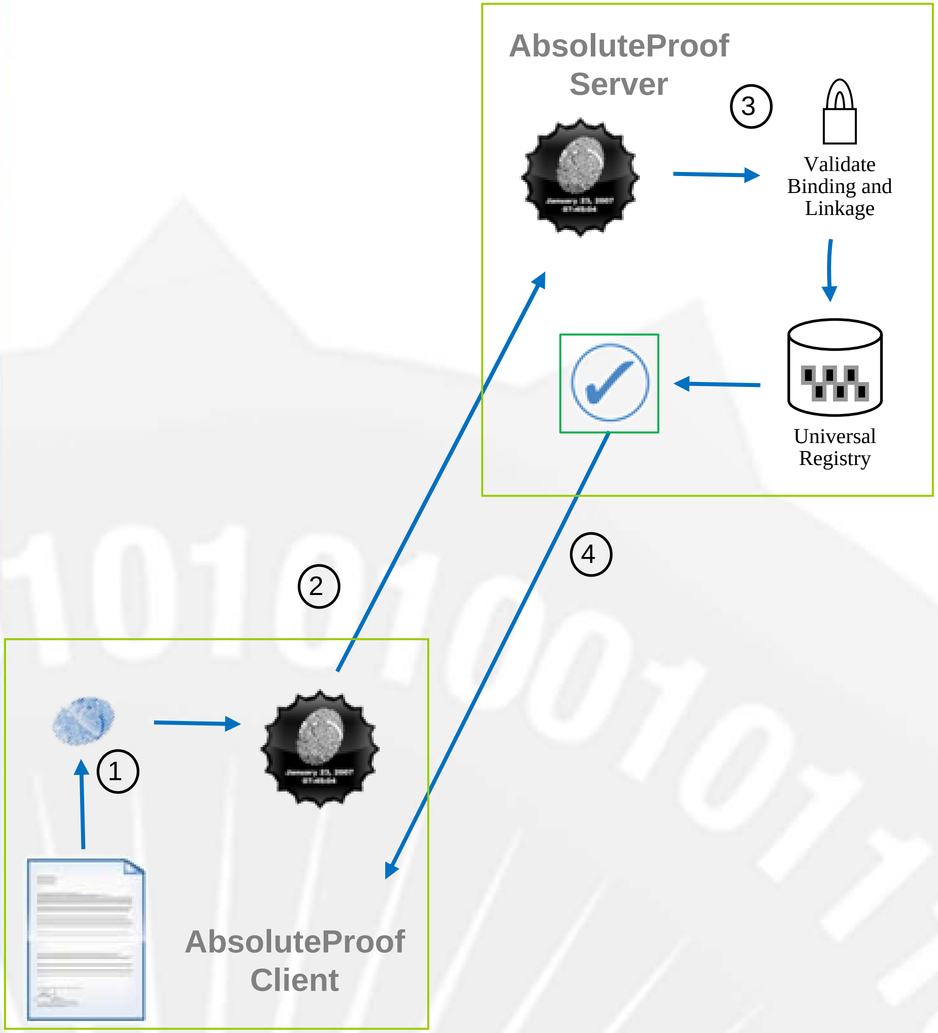
3. AbsoluteProof Server securely and verifiably binds the hash and timestamp to create the Surety Integrity Seal.

4. AbsoluteProof Server sends the Surety Integrity Seal to the AbsoluteProof Client.

5. AbsoluteProof Client securely archives the Electronic Record and associated Surety Integrity Seal.

# AbsoluteProof Service – How We Do It

*Validating the original authenticity of a record*



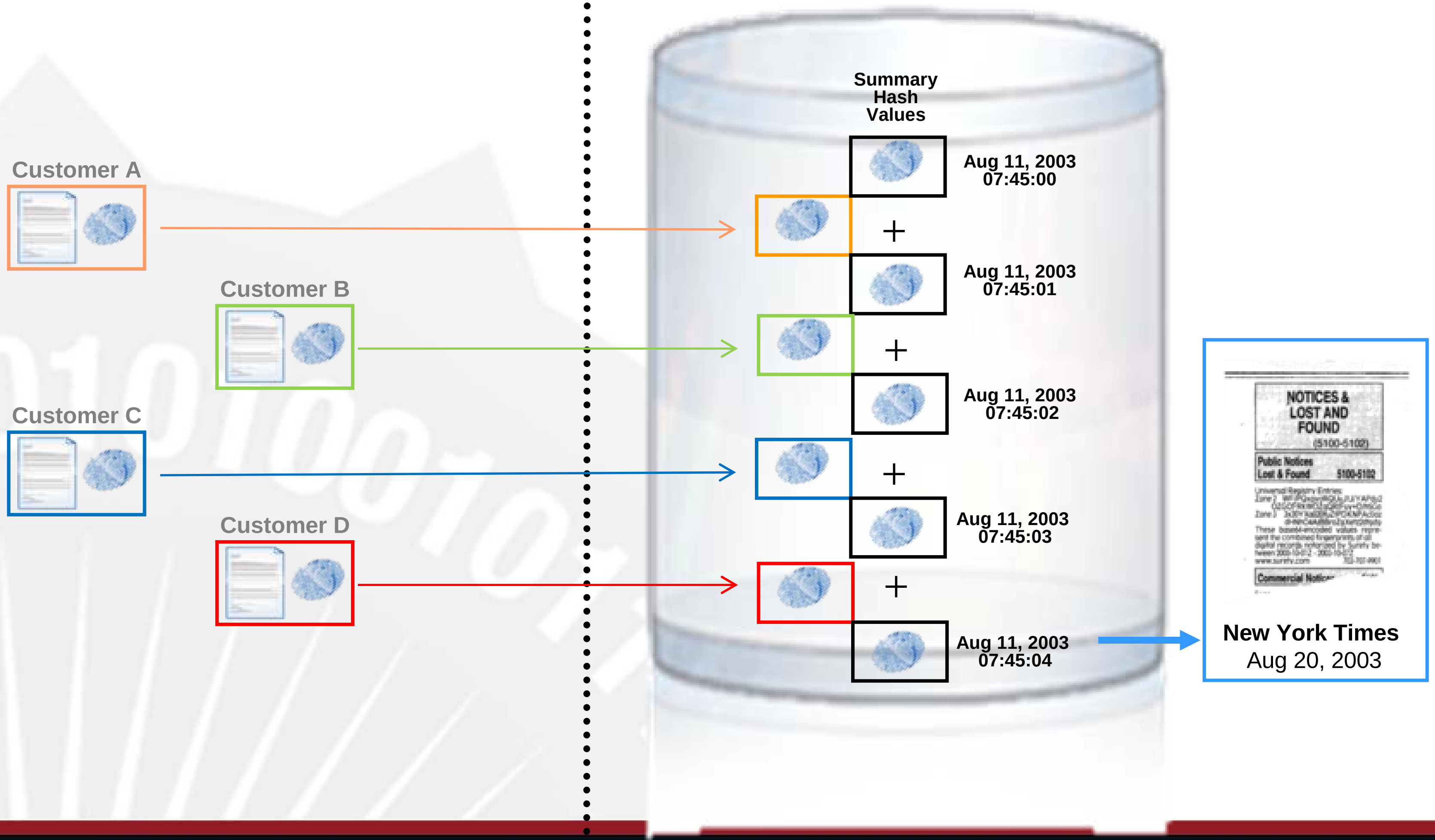
1. AbsoluteProof Client creates a hash of an electronic file, and compares it to the hash stored in the Surety Integrity Seal.
2. AbsoluteProof Client sends Surety Integrity Seal to AbsoluteProof Server.
3. AbsoluteProof Server confirms that both the hash and secure timestamp with the Surety Integrity Seal remain unaltered.
4. AbsoluteProof Server sends a response to the AbsoluteProof Client, indicating validation was successful.

# AbsoluteProof Service – How We Do It

*Hash-chain linking & "widely witnessing"*

## Surety Customers' Internal Systems

## AbsoluteProof Universal Registry Database



# Key Conclusions

- Proving data authenticity is a “bet-the-business” issue
- Amended federal rules and new case law raise awareness
- Corporate risk and economic impact are great
- Lawyers use data integrity challenges as a weapon
- Good people, processes and (compliant) systems, self-managed or in the Cloud, are not enough to withstand a regulatory audit or a legal challenge
- Data security , chain-of-custody and transparency are huge obstacles to broader cloud services adoption
- Enterprise customers can independently prove the integrity of their data when they use trusted timestamps in a self-managed or cloud computing environment
- Cloud Services platforms can use “data integrity protection” and “guarantee” as a key competitive differentiator
- Surety is the only trusted timestamp authority that guarantees the legal defensibility of its service

# Questions – Contact Information

**Tom Klaff, CEO**

tklaff@surety.com

Tel: 571-748-5796

**12020 Sunrise Valley Drive • Reston, Virginia 20191 • Tel: 571.748.5800 • Fax: 571.748.5810 • www.surety.com**