



A Pruvan White Paper

April 2014

## Tamper Proof:

A proposal for an industry proof of performance standard for the property preservation industry



Introduction ..... 3

Proof of Performance ..... 4

*Photo Integrity* ..... 4

*Photo Editors*..... 4

*Date Stamping*..... 5

Exif Data..... 6

*Exif Data – How It’s Recorded*..... 7

*Exif Data – Ease of Editing*..... 8

*Mobile Applications*..... 9

Building Trust ..... 10

    Trusted Devices – Trusted Photo Capture..... 10

    Trusted Storage..... 10

    Verification by Stakeholders ..... 11

    Tamper Proof ID: ..... 11

Tamper Proof Certification..... 12

    Tamper Proof Requirements..... 12

    Tamper Proof Testing..... 12

    Photo Contents..... 13

    Date and Time ..... 13

    GPS Coordinates..... 13

    Trusted Data Transfer ..... 13

    Trusted Storage and Validation ..... 13

The Pruvan Standard for Proof of Performance..... 14

Pruvan Tamper Proof Summary Report Card..... 15

Summary..... 16



## Introduction

Today's mortgage servicers in the property preservation industry face an unprecedented combination of new governmental regulatory and compliance mandates as well as new technological requirements from upstream nationals and banks. New finance reform laws continue to pressure banks and government-sponsored enterprises (GSE's) to provide accurate information about the details of all field servicing activities. This information must be available for audits, months or even years later, to avoid legal risks like penalties or fines.

The basis for proof of performance in the property preservation industry has always been the photograph. Photos can provide clear before, during and after visual evidence that work has been done. The problem with photos is that they can be falsified in many ways. Old photos can be resent as the latest lawn mow. Photos of one house can be substituted for another. Photos can be edited to remove or add debris. Many property preservation companies have "walls of shame" that display falsified photos from vendors who have been caught cheating.

To meet these challenges the industry has responded over time with increasing photo requirements. It has been common for years to require a date stamp to be visually overlaid on the lower right corner of each photo. It is now becoming common to require photos to have Exif based date, time and GPS information. Since jobs are declined for payment if the photo requirements are not met there is a natural incentive to meet photo requirements by any means necessary. Unfortunately the above technologies are also vulnerable to falsification.

Date stamping is easily manipulated with a variety of PC based photo editing and resizing tools. Exif based date, time and GPS information can also be easily altered with both PC and mobile based tools. Photo editing tools have reached new levels of sophistication where any item can be added or removed from a photo with the click of a mouse. All of the above undermines the trustworthiness of photos and calls the validity of the services provided into question.

This white paper focuses on proposing a new industry standard that specifies how photos can be collected in the field to provide true proof of performance that is Tamper Proof. We introduce the concept of the Tamper Proof ID which can be used to recall the photo and verify its authenticity, years after the photo was taken. We will also define Tamper Proof certification requirements that any solution can be tested against to ensure compliance to the standard.

# PRUVAN

## Proof of Performance

As we have stated, the basis for proof of performance in the property preservation industry has always been the photograph. Photos are now required to have date stamps in addition to Exif based GPS and date and time info. Let's look at the detailed vulnerabilities of these approaches.

### *Photo Integrity*

The content of a photo is the baseline of proof of performance. Photos are used to assess the condition of the property before, during and after work is performed. Audits are routinely performed on photographic evidence. Any anomalies, inconsistencies or subjectivity of the photos can result in penalties and fees for years after the work was completed. Unfortunately the content of the photo is not as reliable as we would like it to be.

### *Photo Editors*

The ability to modify or “Photoshop” photos is nothing new, particularly in the property preservation industry. New photo editing features such as “content aware fill” make it simple to make the flamingo on the left of the photo below disappear in seconds. Imagine how easy it is to make trash or debris disappear or increase a cube count. Sophisticated image editing is even available on mobile devices.



*Figure 1. Make a flamingo disappear with the click of a mouse.*



## Date Stamping

Date stamping has been required for years on property preservation photos. Many point and shoot cameras have a feature that will automatically stamp the date onto the photo when it is taken. The problem with this approach is that the camera will allow the user to set the date or time to anything he likes, thus falsifying the photo at the source. There is also an abundance of software that gives the user power to manipulate both date and time stamps to photos after the fact.

To get an appreciation for how common this is, do a Google search on “REO fixing the date stamp of photos.” You will see hundreds of training videos from REO field service companies.

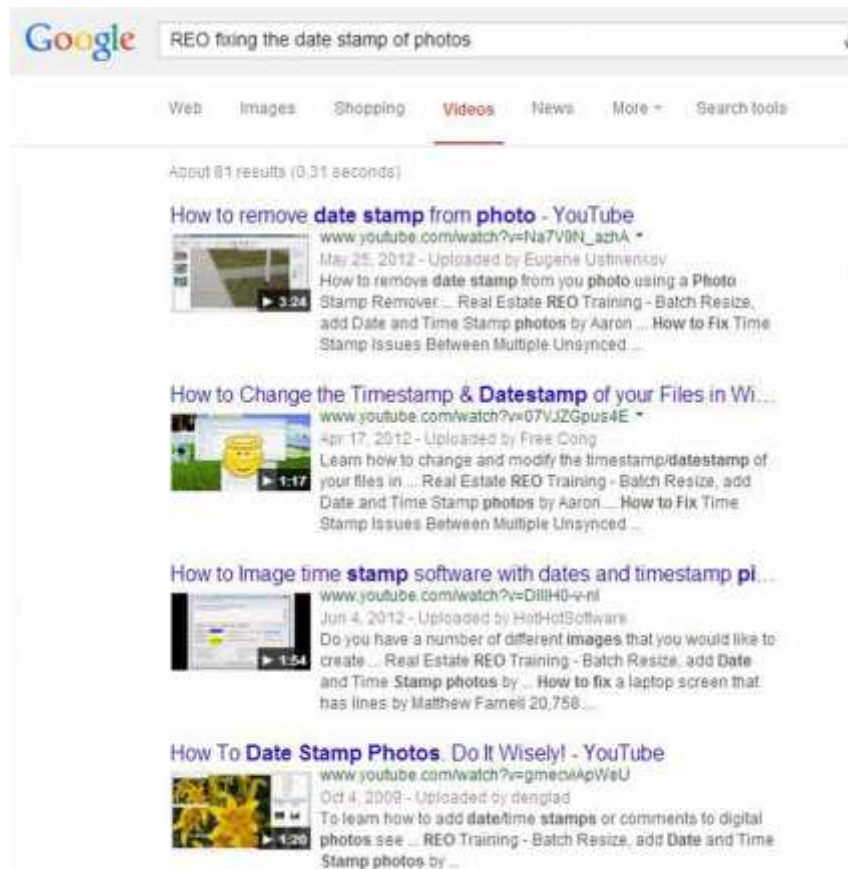


Figure 2. Date stamp editing is commonplace in Property Preservation

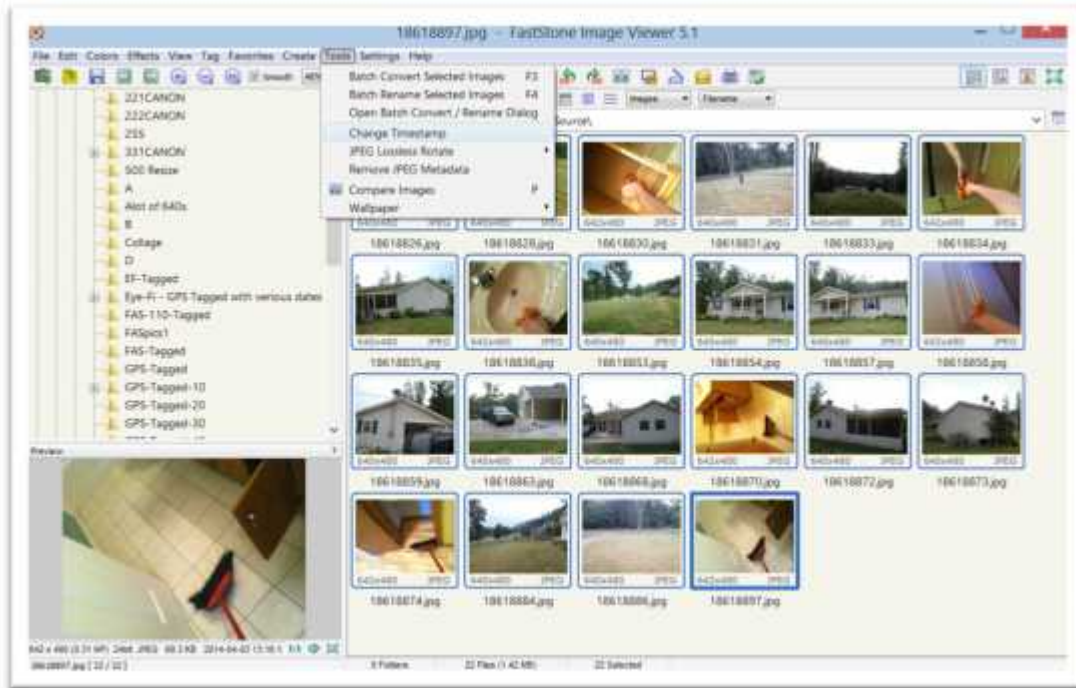


Figure 3. Creating a date stamp after the fact is easy with FastStone

For these reasons date stamping is a completely unreliable way to validate a photo.

## Exif Data

Exif data is now being required by several national property preservation companies. Exif is useful as it is a secondary source of date and time stamp information and can also be used for storing the GPS coordinates of where a photo was taken.

The fundamental flaw in using Exif for proof of performance is how it is recorded and the ease with which it can be modified.



*Exif Data – How It’s Recorded*

Exif data is recorded by the camera when the photo is taken. The camera simply inserts the current date, time and GPS coordinates reported by the device. A photo can be backdated or forward dated simply by changing the date or time on the camera before taking pictures.

Smart phones have a feature that allows the date and time to be set automatically to the ‘network time’ which is always current and correct. Unfortunately this feature can be turned off by the user and the date and time can be easily manipulated.

GPS coordinates are also vulnerable. Android devices have a feature called “Mock Locations” that allow the GPS coordinates of the phone to be set to anywhere the user desires.

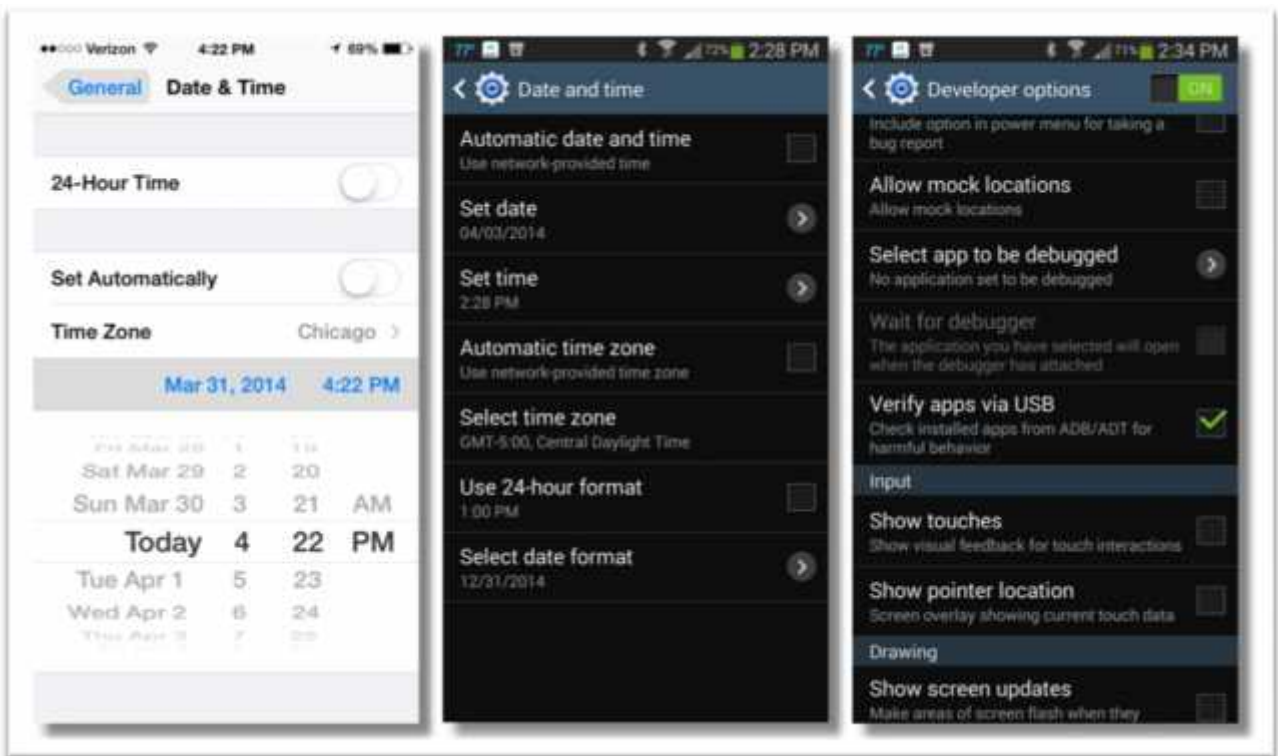


Figure 4. Date, time and GPS location are easily altered on mobile devices



If the date, time, or GPS information has been altered on the device, the camera will happily embed this incorrect data into the photo's Exif data when the photo is captured. Clearly, Exif data is vulnerable at the source device as well.

### *Exif Data – Ease of Editing*

Exif data is stored directly in the photo itself and it can be easily modified. There is a wide variety of Exif editors available on all platforms including all mobile platforms.

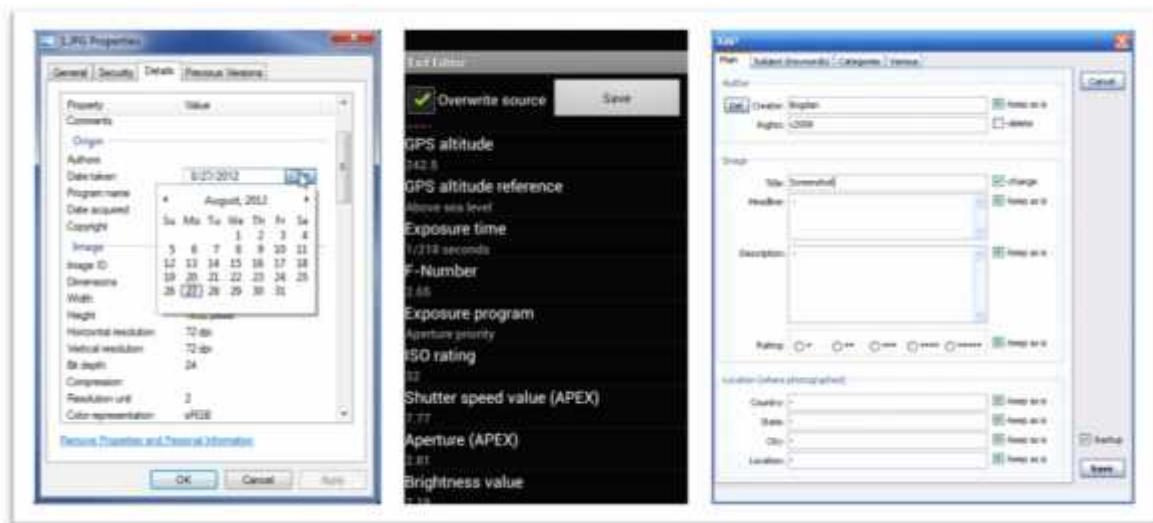
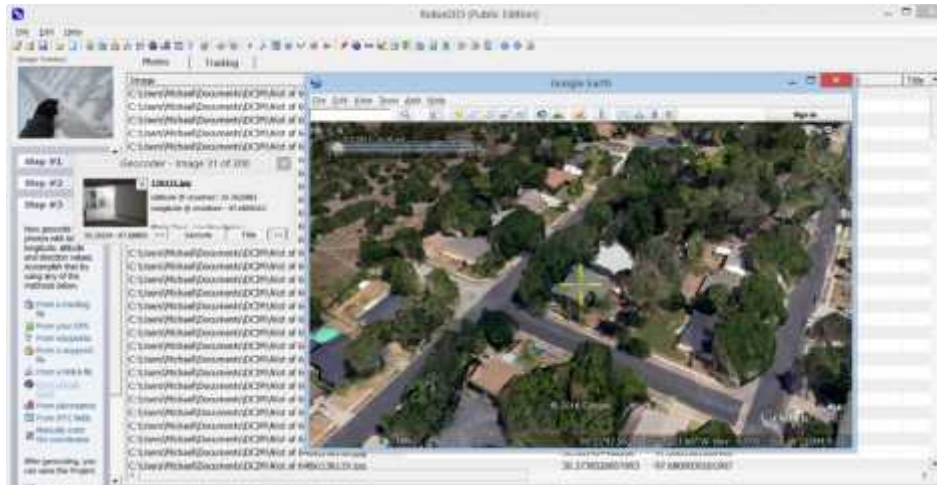


Figure 5. Exif editors in the Windows file manager, an Android App, and MacOS.





Exif editors are legitimately used by photographers to set date, time, and GPS coordinates on photos.



*Figure 6. Updating the GPS Exif info on a batch of photos is as easy as clicking the crosshairs with the RoboGeo PC based application.*

These tools work on entire directories of photos, setting the date, time, and GPS Exif info on each and every photo. It is even possible to set a start date and time and enable the Exif data to embed photos with data over a set period of time. This causes the photos to appear as if they had been taken over that given period of time.

It's common for contractors to forget to set the correct date and time on a point and shoot camera. This happens routinely when a camera runs out of batteries; the clock will typically be set to January 1<sup>st</sup>, 1970 at 12AM. When this happens, all the photos taken with that camera will have the incorrect date and time. It has become common practice in the industry to correct the date and time for this and other reasons, to the point where many work order management systems have built in functionality to reset date and time Exif info.

### *Mobile Applications*

Mobile applications are now becoming commonplace. Mobile apps can improve photo integrity by making it more difficult to access the photo but most mobile apps today do not adequately restrict access to the



photo contents. Photos can still be accessed and altered on the mobile device's file system. Both photo editing tools and Exif editing tools can be used to directly modify photos.

As previously stated, the date, time, and GPS location can be altered on the Mobile device prior to taking the photo. In this case, when the photo is taken, the invalid information will be embedded into the photo Exif data.

Mobile applications by themselves do not provide proof of performance that is tamper proof. Only a mobile application that complies to the tamper proof standard as defined in this white paper can provide proof of performance that is reliable.

## Building Trust

What is required to be able to capture photographic evidence that can be trusted for reliable proof of performance?

### Trusted Devices – Trusted Photo Capture

First and foremost the device capturing the photo must be able to capture the photo in a trustworthy manner that prevents end user manipulation. Smart phones provide a perfect platform for trusted photo capture. Properly written native mobile applications have the required low level control of a smart phone's clock and GPS to be able to capture date, time and location information (photo metadata) in a trusted manor.

### Trusted Storage

Once the photo is captured it must be securely stored. Any modification of the photo contents or photo metadata must not be possible.



## Verification by Stakeholders

Once the photo is captured and stored securely we need to be able to allow stakeholders in the photo (contractors, vendors, servicers, banks etc.) to be able to use the photo as a proof of performance document. This will involve transferring the photo to several intermediate systems for QA, invoicing and auditing purposes. Once the photo has left the trusted repository it is vulnerable to alteration once again.

How can photos be protected and ultimately authenticated throughout the entire value chain? The solution to this problem is the Tamper Proof ID.

## Tamper Proof ID

A Tamper Proof ID is a universally unique identifier or UUID that is assigned and added to the photo as a caption at the bottom of the photo. The Tamper Proof ID identifies the photo as a Tamper Proof photo that can be validated as authentic by any authorized party in the value chain. The Tamper Proof ID consists of a provider code and the Tamper Proof UUID as show below:



Figure 7. The Tamper Proof ID in the format of provider://xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx.



Any authorized party in the property preservation value chain can go to the provider's authentication webpage to validate the picture for at least 7 years from the data the photo was taken. The authentication webpage takes the Tamper Proof UUID as input and then responds by displaying the original photo and where and when that photo was taken.

## Tamper Proof Certification

A mobile solution vendor would be required to pass a certification test to be qualified as a Tamper Proof Photo provider. The certification test would involve testing the vendor's solution to ensure that it can provide the minimum requirements for the Tamper Proof standard.

## Tamper Proof Requirements

- Photos are framed with a Tamper Proof ID (a UUID) at the bottom of each photo.
- Tamper Proof Authentication requires:
  - Ability to absolutely validate the integrity of **photo contents**.
  - Ability to validate and grade **date and time** authenticity and accuracy.
  - Ability to validate and grade the **GPS coordinates**' authenticity and accuracy.
  - Ability to deliver photos and authentication data using a **trusted data transfer** (no undetected end user alteration of photos or data permitted).
  - Photos can be **authenticated for a minimum of 7 years** via their Tamper Proof ID via a disinterested third party Tamper Proof Photo provider.

## Tamper Proof Testing

Tamper Proof testing can be carried out by each Tamper Proof photo provider of their own solution. Results should be publically published to allow peer and industry review. Industry groups could also participate in Tamper Proof testing. Solutions would be evaluated on the following criteria:



## Photo Contents

Once the photo is taken a Tamper Proof solution must be able to detect **any** alterations to the photo. Upon transfer to trusted storage the Tamper Proof solution must identify altered photos and reject them. In no case should an altered photo be accepted into trusted storage.

## Date and Time

When the photo is being taken the Tamper Proof solution must be able to detect if the date and time being reported is from a trusted source (cellular network time or similar). If trusted time is not available the Tamper Proof solution must be able to grade the accuracy of the of the photo time stamp from a trusted source (taken within +/- n hours from a certified time). If a photo is not certifiable the Tamper Proof solution must label the photo as 'not time certified'.

## GPS Coordinates

When the photo is being taken the Tamper Proof solution must be able to detect if the GPS coordinates being reported are from a trusted source (hardware GPS, inaccessible to end user manipulation). The Tamper Proof solution must also be able to grade the accuracy of the GPS coordinates (taken within +/- n distance from target address). If a photo is not taken with certifiable GPS coordinates the Tamper Proof solution must label the photo as "not location certified."

## Trusted Data Transfer

Once the photo is captured on the device the Tamper Proof solution must be able to transfer it to trusted storage and detect any alteration or man in the middle attacks on the data transfer. If the data transfer is altered in any way the solution must reject the transfer. In no case should an altered data transfer be accepted into trusted storage.

## Trusted Storage and Validation

The Tamper Proof photo provider must provide trusted storage for photos and authentication data for up to 7 years and provide authenticated stakeholders access to verify photos via their Tamper Proof UUID.








## The Pruvan Standard for Proof of Performance

Pruvan leads the industry in providing full support for the industry standard for proof of performance. Pruvan provides complete tamper-proof, summary information and verifying authority features that are unmatched in the industry. At the moment each photo is taken it is digitally signed and a copy is immediately uploaded to the Pruvan cloud for verification and storage. The Pruvan Direct mobile app will not allow any photos to be taken if the phone is in airplane mode or if the date and time have been changed. On mobile platforms where it is not possible to detect these details, Pruvan can validate the time within a reasonable time frame (usually a few hours). Any photo that has been altered will be rejected by the Pruvan cloud and not allowed to be sent on to the client. Every Pruvan photo has a unique Tamper Proof ID. With this identifier, any photo taken with Pruvan can be accessed, viewed and audited for authenticity against the photo submitted to the client. Upon completion of a job, a Pruvan Certified Service Record is generated providing a summary of the work performed including a map.



## Pruvan Tamper Proof Summary Report Card

Question	Passed?	Explanation
<b>Photo Contents</b>		Passed. Pruvan digitally signs each photo as soon as it is taken. If the digital signature does not match the photo contents when it is uploaded the system will reject the photo.
<b>Date and Time</b>		Passed. Pruvan does not allow devices to have their time manually set. In the cases of where this detection is not possible Pruvan can reliably verify the time taken within a matter of hours.
<b>GPS Coordinates</b>		Passed. Pruvan detects if mobile devices have their GPS turned off (airplane mode) or if Mock Locations are enabled. GPS authenticity and accuracy are captured and transferred with the photo.
<b>Trusted Data Transfer</b>		Passed. Any alteration of data during data transfer from Pruvan Mobile to Pruvan's trusted storage is detected and the transfer is aborted.
<b>Uninterested Third Party validation for at least 7 years</b>		Passed. Pruvan stores all photos for at least 7 years. All photos can be verified at <a href="https://direct.pruvan.com/verify">https://direct.pruvan.com/verify</a> with their UUID. Pruvan is independent and our business is based on being a trusted and uninterested 3rd party.



## Summary

Today's servicing vendors are under constant pressure to comply with ever mounting technical requirements. This is to ensure that the work being reported is actually being done. Vendors who can provide the highest quality work as well as provide the most accurate data will be the most likely to succeed. Pruvan is the leader in providing the most full featured and robust proof of performance solution in the industry. Pruvan Direct, Pruvan mobile app, Pruvan Certified Service Record and Pruvan's support for the Tamper Proof standard provide a complete solution for an industry proof of performance standard.