Wolters Kluwer

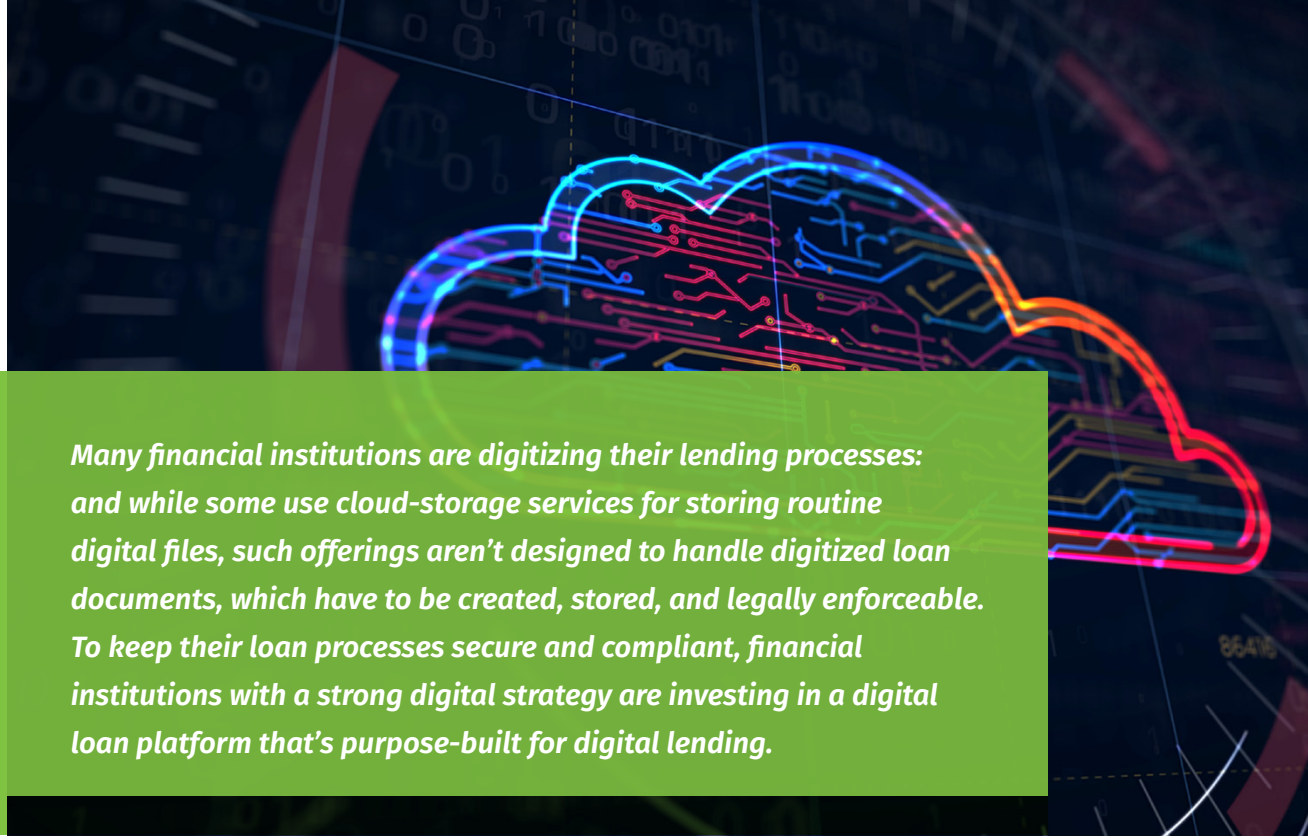
When you have to be right

EXECUTIVE BRIEF

Digitized Loans and Cloud-Storage Services: ***Why Every Bank Needs a Purpose-Built Digital Lending Solution***

eOriginal®

Trust the Asset. Trust the Transaction.®



Many financial institutions are digitizing their lending processes: and while some use cloud-storage services for storing routine digital files, such offerings aren't designed to handle digitized loan documents, which have to be created, stored, and legally enforceable. To keep their loan processes secure and compliant, financial institutions with a strong digital strategy are investing in a digital loan platform that's purpose-built for digital lending.

Financial institutions, like many businesses, are managing more data in the cloud. In the process, their users might save work documents in popular cloud-storage offerings: Box™, Dropbox™, Microsoft OneDrive®, and many others.

But are these services safe? And are they appropriate for storing and managing digitized loan documents?

Virtually all cloud-storage services use data-encryption technology, and some add supplemental security measures. Still, such services might have security shortcomings. For instance, back in 2016 Dropbox revealed that 69 million customer passwords had been compromised.[1] More recently, in March 2020 Data Deposit Box leaked detailed information about 270,000 customer files, along with personally identifiable information.[2]

In April, Microsoft patched a vulnerability that had allowed attackers who gained access to an endpoint to elevate their privileges and use OneDrive to overwrite files.[3] In June, Box was called out for misconfiguring HTTP Strict Transport Security settings, leaving site visitors vulnerable to man-in-the-middle attacks.[4]

And in August, Google revealed a security issue that allowed Google Drive users to upload a new version of an existing file, even if the new version included a malicious executable. As a result, any file that had been shared among users could be replaced by a malicious file – with no indication that changes had been made to the file.[5]

From 'Not Fit for Purpose' to 'Purpose-Built'

But when it comes to digitized loans, there is an even bigger issue: Simply put, generic cloud-storage offerings aren't designed to support digitized lending processes. In particular, they aren't intended to meet the legal, regulatory, and security requirements of an end-to-end digitized workflow. The result? Unacceptable risk, noncompliant process steps, and unsatisfactory customer experiences.

Financial institutions that want to avoid the limitations of generic cloud storage and gain the power of a purpose-built solution should understand these six truths of digital lending:

1 *Digitized lending requires a solution that overcomes the legal, compliance, and security shortcomings of generic cloud-storage offerings*

Cloud-storage services are designed to store digital assets, and to do that securely. But a digitized loan is more than just a simple document. It's a financial asset that has underlying real value, and requires much more than just protection against data leakage in order to be compliant and legally enforceable.

Various regulatory bodies, from the Federal Reserve to the Small Business Administration, specify rules for how loan documents are stored. Financial institutions need to be able to demonstrate that loan documents were created with the consent of both parties, that they were not altered without a record of that alteration, and that they are auditable throughout their lifecycle.

Generic cloud-based storage services are not intended to store digitized loan documents in this way. Although they might allow users to share documents with version control, they do not provide for auditability or capture the ancillary data needed to maintain a negotiable and enforceable financial instrument.

2 *Regulatory compliance is a requirement of digitized lending*

Key pieces of legislation – such as the Uniform Commercial Code section 9-105 (UCC 9-105), the Uniform Electronic Transactions Act (UETA), and the Electronic Signatures in Global and National Commerce Act (ESIGN) – establish rules for recognizing electronic records on an equal basis with paper records. For digitized loans to be enforceable and negotiable, they need to comply with these laws.

If a financial institution wants to originate loans that can be bought and sold by third parties, those loans need to be unique and identifiable negotiable instruments. That ability demands a system that provides an auditable chain of control and custody. Such a capability gives you a "digital original" document – a single, authoritative copy with all the legal rights of a paper contract.

Digital Lending and Regulatory Compliance

Two crucial aspects of an eRecord – such as a digitized loan – include ensuring an authoritative copy and establishing control. "Control" is to the authoritative copy what "possession" is to a paper security.

Federal laws require control of the authoritative copy by a system that reliably establishes a party is assigned, issued, or transferred the authoritative copy. Relevant legislation includes:

- **Uniform Electronic Transactions Act (UETA) of 1999**
  Proposes uniform rules for states to treat electronic signatures as legally equal to "wet" ink signatures
- **Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000**
  Authorizes the use of eSignatures for transactions between parties in all jurisdictions where federal laws apply
- **Uniform Commercial Code Section 9-105 (UCC 9-105)**
  Specifies that a secured party has control of eChattel, if a system used for evidencing transfer of interests in the eChattel establishes the secured party as the person to which the eChattel was assigned

UCC 9-105 also requires that the authoritative copy be created, stored, and assigned to meet six stringent Safe Harbor Provisions:

1. **Authoritative copy** – The availability of a single, authoritative copy that is unique, identifiable, and unalterable.
2. **Assignee identification** – The authoritative copy identifies the secured party as the assignee of the record or the person to which it was last transferred.
3. **Communication and maintenance** – The authoritative copy is communicated to, and maintained by, the person asserting control or the designated custodian.
4. **Secured party modification** – Revisions that change an assignee must be made with participation of the person asserting control.
5. **Copy identification** – Any copy that is identifiable as not the authoritative copy.
6. **Copy revisions** – Any amendment is identifiable as either authorized or unauthorized.

3 *Digital asset protection is about more than just confidentiality*

Loan documents must be not only encrypted but also tamper-sealed. If your financial institution plans to sell loan assets into the secondary market, you must be able to demonstrate that a loan document that says it represents a property valued at $500,000 actually does so. The document needs to be tamper-sealed such that all actions against the document have been digitally recorded, and there were no changes to the document between the times when it was signed and it was sold.

4 *"Digital Asset Certainty" should be central to your digital lending strategy*

Digital Asset Certainty is a concept enabled only by eOriginal® solutions. It provides the assurance that your digital loans are compliant and meet all legal requirements and industry best practices. Digital Asset Certainty gives you an auditable, tamper-proof digital chain of custody for your digitally originated loans, plus the legal standing that shows these loans comply with all applicable laws.

As a result, you gain a digital original that guarantees the asset is the authentic, authoritative copy. As that digital original moves through the lending ecosystem, an immutable, evidentiary trail of ownership is captured, with each participant's involvement serving as a record of the loan's history.

5 A purpose-built solution is crucial to digital lending

Cloud-storage services are designed simply to store documents. They are not intended to meet the regulatory and legal requirements of digitized loans. For example, they don't meet the UCC 9-105 Safe Harbor criteria, including ensuring an authoritative copy, assignee identification, and copy identification. Only a digital solution specifically designed to support the end-to-end loan process, from origination to sale into the secondary market, can do that.

Encryption prevents unauthorized users from seeing the data. But that's only one aspect of asset management of a digitized loan document. You must also be able to demonstrate that the document hasn't changed – or if it has changed, who changed it, when it was changed and how it was changed. The file needs to be tamper-sealed, and it needs to be recorded in an audit trail that itself is tamper-sealed.

End-to-End Digitized Lending

A purpose-built digital lending solution addresses the needs of all stakeholders through every phase of the lending process, from origination through sale to the secondary market.

6 A purpose-built solution ensures digital asset certainty, regulatory compliance, and security through every phase of the loan lifecycle

Many financial institutions don't hold the loans they originate. Instead, those loans are packaged and securitized. A single, purpose-built platform enables institutions to manage the process from end to end, from origination to sale into the secondary market.

Lenders must keep in mind that investors don't buy a single auto loan, but an aggregation of thousands of auto loans: this means financial institutions must ensure that those loans were originated, aggregated, and transferred as a bundle with a single element of control. To protect their assets, they need a solution designed for that purpose.

A purpose-built solution is the foundation of digitized lending. By investing in a purpose-built platform at the beginning of their digital journey, financial institutions gain the compliance and security that enable an optimized digitization strategy.

Finally, leveraging a purpose-built digital lending solution delivers benefits beyond just compliance and security. It allows borrowers and every other stakeholder in the loan process to benefit from digitization. It provides the capabilities that enable secure and compliant digitized loans, and it delivers customer experiences that enable financial institutions to differentiate themselves in the marketplace and grow their business.

[1] *"It's Official: 69 Million Dropbox Accounts Leaked," Infosecurity Magazine, August 2016*

[2] *"Data Breach Report: Cloud Storage Exposes 270,000 Users' Private Information," Security Magazine, March 2020*

[3] *"Windows OneDrive Security Vulnerability Confirmed: All You Need to Know," Forbes, April 2020*

[4] *"Are Cloud Storage Providers Dropping the Box on Security?" Upgard, August 2020*

[5] *"A Google Drive 'Feature' Could Let Attackers Trick You Into Installing Malware," The Hacker News, August 2020*

eOriginal®
Trust the Asset. Trust the Transaction.®

250 W. Pratt Street,
Suite 1400
Baltimore, MD 21201

Contact Us at
1-866-935-1776

Please visit **www.eoriginal.com** for more information.