

Global Banking Group Secures Sensitive Customer Information via FileCloud

case study



Global Banking Group Secures Sensitive Customer Information via FileCloud

Our client is a highly respected, trusted, and historic large corporation in the banking, financial services, and insurance (BSFI) sector. Originally founded in the early 19th century, it is among the top 60 banks in the world. Additionally, it is in the top four financial institutions within its own geographical region.

An organization with various complex lines of business, the sharing of personally identifiable information (PII) and other sensitive data is an integral part of its daily operations. For this institution, complying with intricate data security and regulatory requirements, while still remaining operationally efficient, is vital. In addition, regional regulations mean that adherence to data residency requirements is non-negotiable.

The group also has a strong wealth management division, which provides investment, pensions, and insurance products. It's no exaggeration to say that this multinational organization plays an integral role in keeping the fabric of society functioning in the areas in which it operates.

Though largely concentrated in one geographical region, the banking group has offices and operations throughout the globe. It is a member of the Global ATM Alliance, which is a group of highly established, high-street banks across the world that allow customers to use their ATM cards while travelling abroad at member banks, incurring no additional fees.

Each day, this institution services millions of consumers in its B2C lines of business. Its B2B operations provide various vital financial products to:



Small to medium sized enterprises



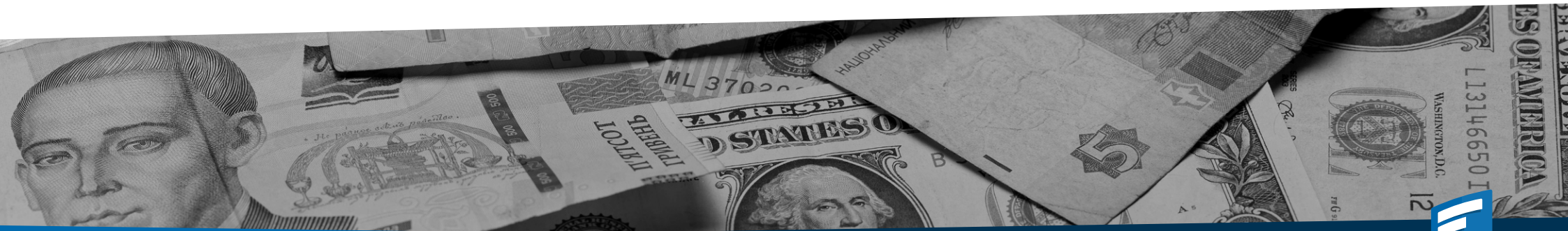
Commercial organizations



Agribusiness customers



Government



Challenges: Combining the Old with the New

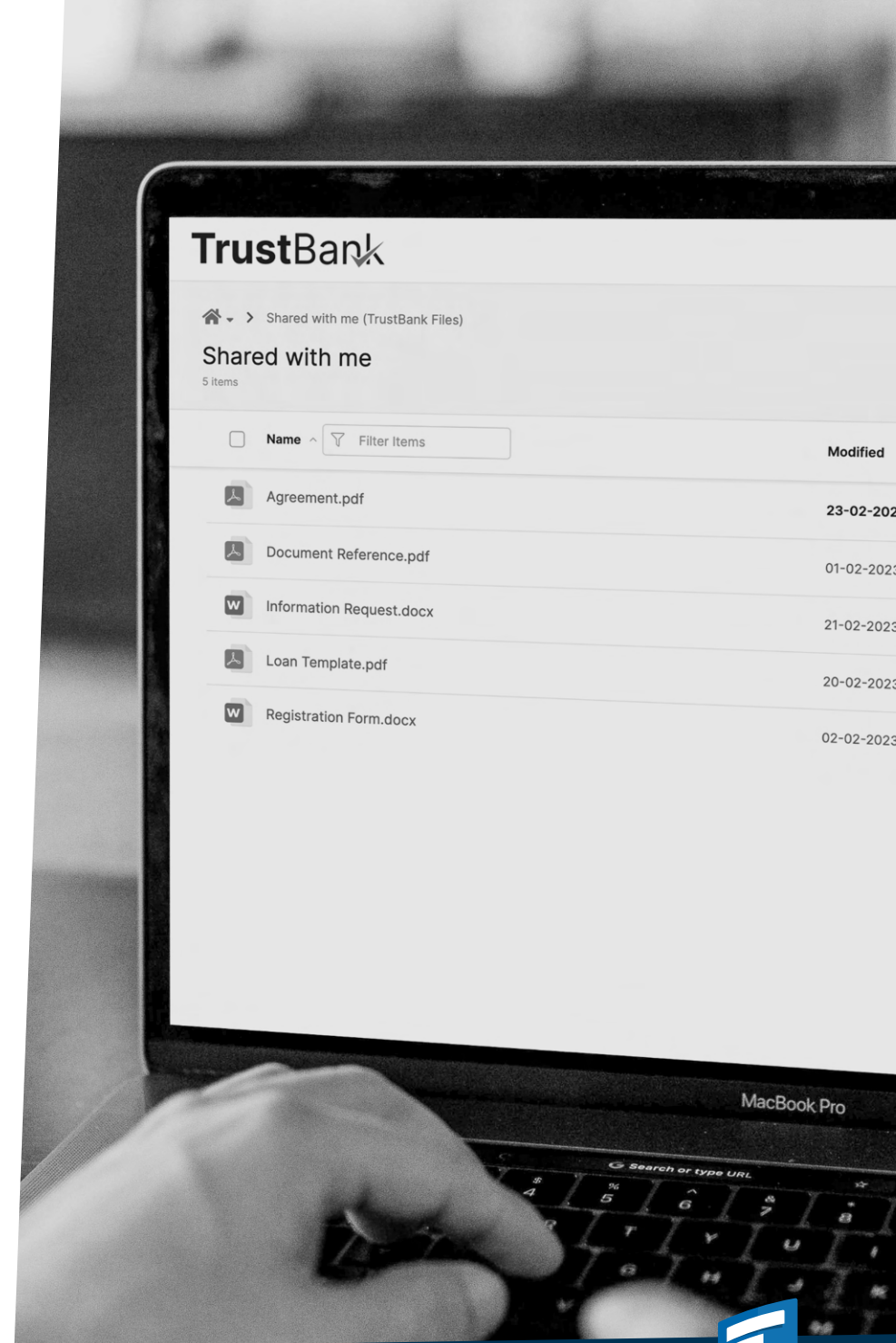
Like many financial institutions, our client saw the potential benefits of digitization while many other sectors were still resolutely paper based. It adopted banking software to streamline processes. As various early adopters of such software are currently realizing, however, legacy technology stacks can sometimes have attack vectors that leave organizations vulnerable to bad actors. Our client was concerned that at some point, the sensitive data being handled and shared on a large scale by the bank could become compromised by the rapidly escalating volume and sophistication of cybercriminals across the globe.

Traditional high-street banks have a strong relationship of trust with customers, and our client was intent on making sure that relationship was honored. This meant doing everything necessary to protect the privacy and integrity of customer data.

Requirement for a Seamless Transition

Although the banking group wished to upgrade its systems, it knew this project had the potential to become challenging. Banking personnel wanted to limit the amount of disruption to both customers and staff that might potentially be involved in a complete system overhaul.

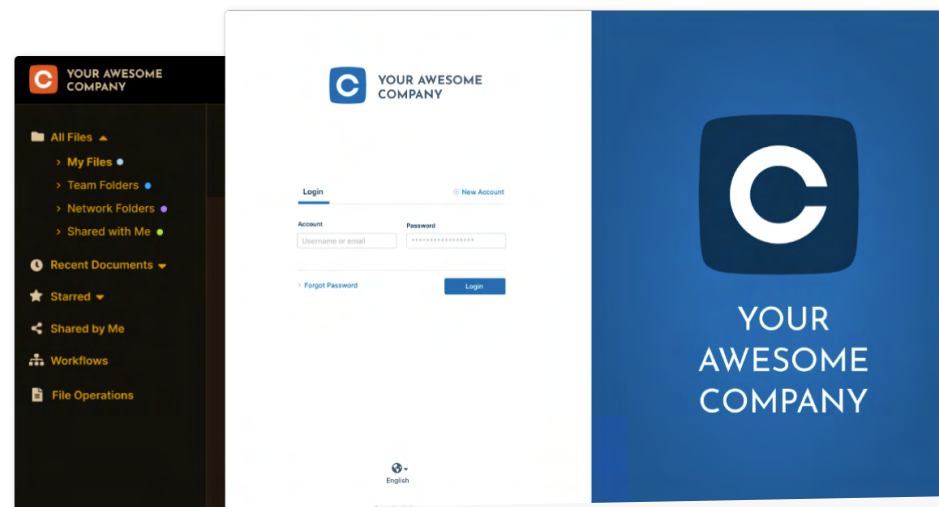
With 13 million customers and around 40,000 staff, it was important that the implementation of a secure content collaboration solution caused minimal disturbance to business as usual. This is why one of the banking group's various requirements was that the solution had to be flexible enough to integrate with the group's authentication directory, SSO, and banking platform.



Customization to Maintain a Group of Trusted Brands

Our client is the parent institution for several banks with their own unique branding requirements. Although existing under one umbrella, the banking group needed a solution that would allow for customization, so that each organization could communicate using its own distinctive corporate identity via logos and URLs.

The flexibility to customize for proper branding is a vital aspect of maintaining relationships of trust with customers in a world with increasingly polished phishing scams targeting customers and financial institutions alike. All measures taken that signify communications are coming from trusted sources are valuable in this context. For this reason, any solution for data sharing within the banking group needed to fulfill multi-tenancy requirements.



Tackling Unsecured File-Sharing

The file-sharing practices within the banking group were not secure enough to provide adequate protection against future cybercriminals on the hunt for valuable data. For example:

- **Zip files** were being shared via group email.
- **Proprietary information** was being sent to outside partners physically on encrypted USB devices.
- **Policy information** was being sent by the life insurance part of the business to reinsurers via CD.

Although files were usually encrypted in these instances, the methods were often time-consuming and cumbersome. Additionally, the level of security was not enough to deter the sophisticated type of cybercriminal we increasingly see today. Our client was aware of the need to remain ahead of the curve on security to protect what was often extremely sensitive data, both at rest and in transit. Future-proofing and streamlining both the B2B and B2C file-sharing practices throughout the entire group had become non-negotiable.



Why Choose FileCloud?

Traditional, high-street banking as we know it today is an age-old industry, with many aspects of current practices dating back to Renaissance Italy. Like many highly established social institutions, its deeply ingrained working practices can be slow to embrace change. Our client needed a file-sharing platform that could integrate with much older software, while also providing state-of-the-art security capabilities to safeguard vulnerable, dated systems and prevent them from becoming obsolete.

Our BSFI client performed careful due diligence, exploring the features of various well-known public file-sharing platforms. With 40,000 staff and millions of customers, care and precision in choosing a solution were especially vital. The banking group settled on FileCloud after finding out about its flexible integration and security capabilities and world-class support.

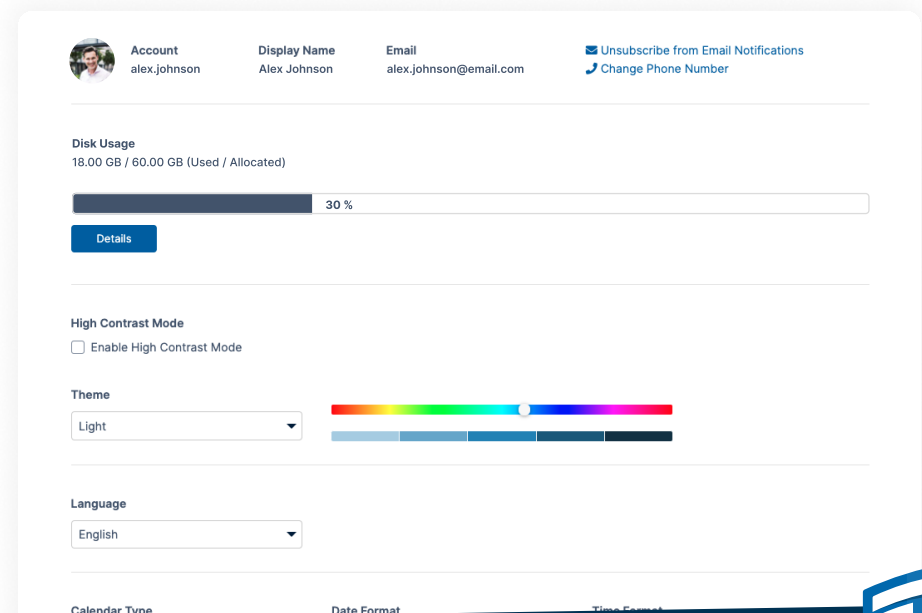
Eminently Scalable Solution

The banking group planned to host 20,000 staff users in the initial phase of the project, with the intention of scaling to 40,000 in a later phase. On exploring available options, banking personnel were confident that FileCloud could achieve these objectives. The fact that that FileCloud's API was flexible enough to integrate with their banking platform, causing no disruption to users, was in itself a huge win to our client.

Prioritizing Brand Recognition

Those involved in due diligence realised that FileCloud could help all banks under its jurisdiction to ensure that both staff and customers could exchange sensitive information securely and efficiently, while also working within reassuringly familiar user environments. The relevant branding for each financial institution could be made visible throughout the customer experience, due to FileCloud's extensive and adaptable white-labeling functionality.

FileCloud's multi-tenancy capabilities would allow them to create a site for each bank. External file-sharing could be done via the brand-specific URLs, due to FileCloud's customization capabilities. The scalability of FileCloud meant that each bank was free to grow as necessary by simply adding users to the relevant FileCloud instance.



Seamless Content Classification & DLP Capabilities

During due diligence, it was important to our BSFI client to settle on a solution that allowed every file to be analyzed to ensure that sensitive information was processed and shared only by authorized people in pertinent contexts. They discovered that FileCloud is integrated with OPSWAT On-Premises DLP, which classifies documents that are used in DLP rules.

As with many banking organizations, our client routinely processes various categories of PII and other sensitive data. The ability to run hundreds of classifications was a vital part of what made FileCloud an attractive solution.

Audit capability and integration with SIEM were also major draws for our client. With FileCloud, every user action can be monitored on SIEM, and an alert raised in the event of unusual activity. A further layer of security was FileCloud's facilitation of controlled workflows, whereby certain files could be shared only after review by a relevant manager.

For these and many other reasons, they chose [FileCloud Server](#), the self-hosting, hyper-secure private cloud solution, over all the other competitors they investigated in the field.

The screenshot shows a 'Rule Update' dialog box with the following fields and options:

- Rule Name:** Client PII
- Affected User Actions:** SHARE
- Rule Expression:** Includes a 'Rule Expression Builder' button and a 'Rule Expression Text Editor' button. The expression is `_metadata.exists('cce.pii')`.
- DLP Action:** DENY
- DLP Mode:** ENFORCE
- Rule Notification (optional):** File contains Client PII - Sharing is not authorized.

At the bottom, there is a 'Rule Creation Help' link, a 'Cancel' button, and an 'Update' button.

The Outcome: An Enterprise-Grade Solution

It took a couple of months to get FileCloud up and running throughout the enterprise. The project began with 5,000 FileCloud users, increasing to 20,000 within a year. The ongoing goal is to scale up to 40,000 users. The banking group had some requests for additional feature integrations, which FileCloud delivered.

FileCloud also trained designated system owners to provide enterprise-wide training to users. Our first-class support team provided ongoing resources and documentation to facilitate this onboarding process.



Transient File-Sharing Requirements

Transient file-sharing is a common practice in our client's financial institution. It is regarded as another method of securing customers' personal information. It also helps minimize the amount of data held by the organization and ensure that it is retained only for as long as is necessary to do so for business purposes.

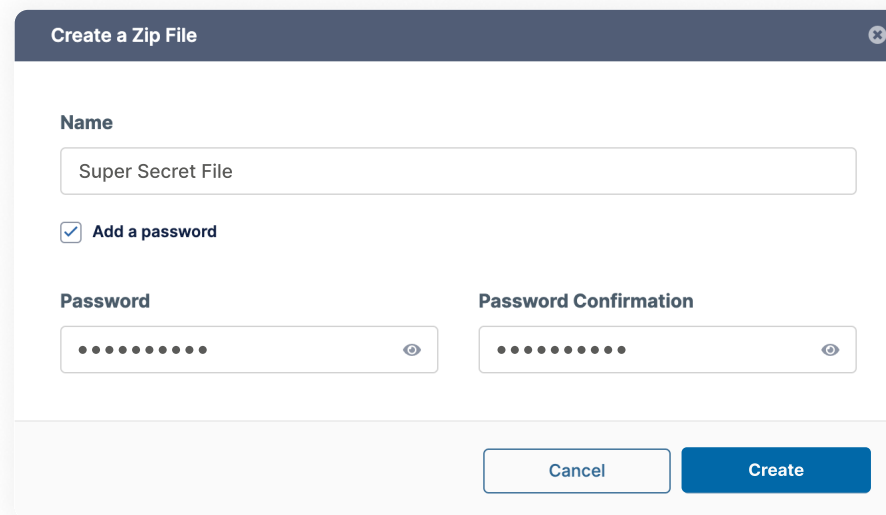
FileCloud's Retention feature is routinely used throughout our client's banks to help them to meet regulatory demands related to data privacy, through automation of data retention and erasure policies.

Zero Trust File SharingSM Capability

FileCloud's support also involved the integration of [Zero Trust File Sharing](#), an invaluable resource when sharing sensitive information.

This allows a customer to access an encrypted archive in the event, for example, of their banking details being stolen by a hacker.

With FileCloud's Zero Trust File Sharing, a hacker would be unable to access the contents of Zero Trust archive, because the passcode is not stored within the FileCloud system. It is only available to the customer via trusted bank personnel. These granular-level, Zero Trust security practices are the future of cybersecurity and provide the bank with alternatives to more traditional perimeter-based methods of securing data.



The screenshot shows a 'Create a Zip File' dialog box. The title bar reads 'Create a Zip File' with a close button. The main content area includes a 'Name' field containing 'Super Secret File'. Below this is a checked checkbox labeled 'Add a password'. There are two password input fields: 'Password' and 'Password Confirmation', both containing masked characters and having an eye icon to toggle visibility. At the bottom right are 'Cancel' and 'Create' buttons.



A Secure, Future-Proof Model for Protecting Customer Data

On 15+ servers, thousands of banking group employees now use FileCloud across several banks, and within the governing banking group to share files. Using FileCloud's enterprise-grade solution, they serve the financial needs of millions of customers. All inbound and outbound file collaboration is facilitated by FileCloud.

In fact, when renewing their contract with FileCloud after four years, all of the necessary documentation was shared by the client using FileCloud itself! Our file-sharing solution is now intrinsic to how this banking group conducts its business operations across the board. This is because our client is secure in the knowledge that FileCloud has conducted multiple security checks before any file sharing takes place. Role-based access control also ensures that collaboration only takes place in the organization for authorized, valid business purposes.

FileCloud has helped this global banking group to:

- Give customers, partners, and staff a **great user experience**.
- **Protect the confidentiality and integrity of data** throughout its banks at all times.
- Prevent unauthorized distribution of **sensitive information**.
- **Enable monitoring of sensitive information** being shared outside the organization.
- Use robust **reporting capabilities**.

Try FileCloud Now

FileCloud's extensive functionality, ease of use, affordability, and world-class support make it the solution for file share, sync, and mobile access already adopted by enterprises and organizations around the world.

You too can benefit from FileCloud and its industry-leading quality and performance today!

Take advantage of [FileCloud's free trial \(15-day online or 30-day server\)](#) and see how FileCloud can help your organization thrive by supercharging content collaboration and processes.

REGISTER NOW

FOR A FREE 15/30 DAY TRIAL,
CANCEL ANYTIME

GET A DEMO

COMPLETELY FREE,
NO STRINGS ATTACHED



Summary

To compete in today's fast-paced market, companies need to get business done without being slowed down by IT challenges. We understand this. FileCloud's software is a solution focused on enterprise file sharing that is just as helpful to business practices as it is to IT requirements.

- Integration with existing resources helps lower business operating costs
- Extensive feature-set and ease of use helps increase user productivity
- Support for an ever-increasing reliance on a mobile workforce keeps you competitive.

FileCloud offers an Enterprise File Sharing and Sync (EFSS) solution that enables you to realize the benefits of collaboration and productivity with the security you require to protect your Intellectual Property anywhere it goes in the course of doing business.



To read more about how FileCloud can secure your information and support collaboration, visit www.filecloud.com/enterprise-file-sharing

"You're the best vendor we've ever worked with, and we measure other vendors based on FileCloud standards. When we ask for something, FileCloud doesn't ignore it. They take the time to go through the problem raised and see if they can find a solution. "

- Project Manager



About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.



1M+
USERS



3000+
ENTERPRISES



100+
RESELLERS



90+
COUNTRIES



13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

CONTACT US



US Army Corps
of Engineers



Deloitte.

Copyright Notice

© 2023 FileCloud. All rights reserved.

No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

