**Couchdrop**

# Managed File Transfer for Banking and Financial Institutions

# Contents

# Overview

With some financial institutions and banks having to protect enormous amounts of financial information–including private customer details and records–security is paramount, more so than perhaps any other industry. Data breaches can lead to compromised records or worse, and as a result, financial institutions have some of the most robust security in the world.

However, as advances in technology have led to the digitization of files and cloud computing is becoming the norm, are banks and financial institutions able to take advantage of these benefits while ensuring their data stays safe and secure?

This white paper will cover challenges financial institutions should take into account when considering cloud computing and file transfers between different platforms. It will also discuss the importance of cybersecurity and how Managed File Transfer (MFT) can help banks and financial institutions overcome obstacles in file transfers.

# Challenges for Financial Institutions

When it comes to file transfers, banks and financial institutions have three important obstacles to overcome. The first is security and ensuring that files can't be intercepted by bad actors. Second is that files can be accessed on the systems where they're needed. And third is that files are transferred reliably as expected.

### Security

Security is important for any organization, but financial institutions need to take extra precautions to make sure their files and assets stay safe. This pertains to file transfers as well. File transfers must be done in a way where the file can't be read or intercepted by anyone except for the intended recipient.

See the later section on Cybersecurity for more detail about security for file transfers.

### Accessibility

If transferring files between systems is an important part of workflows, it's less useful if there is trouble accessing files on the destination. Balancing security and accessibility can be a challenge.

For instance, some file transfer platforms can't encrypt files, but they can send the encrypted files. The file will then need to be decrypted at the destination or run through a decryption program and will be inaccessible until this process is done. Some managed file transfer platforms, however, can both encrypt and decrypt files without the need to access a different external system for increased accessibility.

### Reliability

A secure and accessible file transfer system is useful in theory, but if it's unreliable it won't be of much use. Customers or organization leaders needing to see information about their financial data can't afford to have it unavailable when they need it most due to bugs in the system. Unreliable access can cause trust issues not only in the transfer protocol but also in the institution itself.

# Finance and the cloud

For both customers and employees of financial institutions, keeping data safe is absolutely essential. But in today's collaborative workspaces where the best talent can be distributed at locations around the globe, can banking stay secure and work collaboratively with cloud-based systems at the same time?

The growth of cloud-based banking software proves that financial institutions can work in the cloud, but it's important to keep cybersecurity best practices in mind.

### The rise of cloud banking

Like with other industries, banking is seeing an uptick in platforms that are partially or entirely cloud-based. Alkami, Finastra, NetSuite, and SYSPRO are partially or fully-cloud based, and have increased adoption each year.

These cloud banking application suites have several pieces of software that can handle transactions, customer data, forecasting, and more. They are also regularly updated and bring in new features. While some of them include cloud storage, that storage won't be as versatile or robust as dedicated cloud storage like Dropbox.

They are also meant to work as replacements for existing software, so may not integrate well with systems outside of their application suite, which can be problematic when the legacy systems are still needed.

### Combining on-premises systems with the cloud

Integrating the cloud with on-premise systems isn't always straightforward, especially with legacy systems that were never designed for the cloud. Forcing these to adjust to new functionality isn't always feasible, and sometimes it's better in the long run to switch to a more modern application suite.

A common solution is to use a hybrid of cloud and on-premise systems. Software that processes and houses banking and transaction data can be secure and on-premise. Meanwhile, files used in departments like marketing can make use of collaborative cloud platforms like SharePoint or Google Workspace. Although it may seem like there may be minimal overlap between the two storage options, having a way to send files between on-premise and cloud platforms is beneficial and can be a valuable way to transfer important files.

# The Importance of Cybersecurity

Ever since banks became commonplace, they've been a target for anyone trying to get money fast. As new technologies emerge, financial institutions have found better ways to protect funds, leading to bank robberies becoming increasingly less lucrative–and less common.

Although physical bank robberies have been on the decline, this doesn't mean that bad actors aren't trying to get rich quick off stealing from banks. Just as bank security measures improve, bank thefts have become more sophisticated as well.

### Bank robberies vs cyberattacks

According to a Kaspersky report on malware attacks released in 2022, corporate users are becoming increasingly targeted by malware attacks, rising from under 25% of attack attempts in 2018 to nearly 38% in 2021. And many of those that are successful have huge losses, like the Bangladesh bank heist of 2016 where about $86 million was stolen through a malware attack on the SWIFT system.

Compared to what the average bank robber gets away with–estimated to be under $5000 in 2019–cyberattacks can be much more financially devastating than a robbery. This means that financial institutions can't afford to take cybersecurity lightly

### Avoiding cyberattacks is impractical

With institutions around the world being hit with attempted attacks, completely avoiding cyberattacks is practically impossible–especially with many attack attempts being done by bots.

Instead of aiming to avoid cyberattacks, financial institutions should be aiming to protect data. In 2023, cybersecurity experts suggest overprotecting the most important data by adding additional safeguards whenever feasible so that even if someone gets into the system, they won't be able to steal the most valuable data.

### What does cybersecurity include?

Cybersecurity is an overarching term for protecting digital devices and data. A common usage is referring to antivirus software, but that is only a small portion of cybersecurity. It involves software, but also how devices connect to each other, and crucially, how devices and data are accessed.

Part of cybersecurity includes the way that employees send and access files, and one that is often overlooked. In fact, according to a Clearswift report on cyberattacks in finance, the most common data breaches are a result of employees not following proper security protocols. Note that it's not necessarily

the security protocols themselves that are the issue; employees aren't following proper procedures instead.

## Why do employees not follow security protocols?

Strong security has little use if the protocols are not being followed. When security protocols are robust enough to prevent cyberattacks, why do some employees not follow them? According to Harvard Business Review research on employees violating cybersecurity policies, the top three reasons were inefficiency, inconvenience, and helping others do their job.

Inefficient and complex protocols are ones that seem to get in the way of an employee doing their job. They can be anything from multifactor authentication, processes that require several steps, generating unique access keys per access, and so on. If the process becomes too complicated, employees may avoid some parts of the process when it is in their power to do so, especially if they believe their access carries little risk.

Inconvenience is another major factor. A specific device at a single location might be the only one with the required security software, or an employee may require approval from a specific supervisor to access certain files. If that supervisor is unavailable, for example, the employee might search for a workaround to access the data.

Helping others do their jobs properly can include working with employees who haven't been trained properly, or who haven't received proper authentication for an assigned task. Strong security policies do little good if the people that should be using them are unaware of how to do so, or were never granted proper credentials.

## How often should security protocols be reviewed?

Security protocols that are considered strong at one point may not be as effective in the future. This is because cyberattacks are constantly evolving, as well as security software to help combat them. So how can financial institutions ensure cybersecurity is up to date?

Security protocols should be audited by a third party regularly. For banks and financial institutions, this should be about quarterly, but doing these audits on a more frequent basis can ensure security protocols are able to safeguard from the most recent threats. The audit may reveal new vulnerabilities that can be mitigated before a cyberattack takes advantage of them.

For file transfers specifically, using a Managed File Transfer platform can help reduce cybersecurity risks from moving files.

# What is Managed File Transfer?

Managed File Transfer is a centralized hub that moderates files sent between different systems. It works to consolidate transfers and regulate security protocols between these systems, while providing a central location that all file transfers must pass through.

Through an MFT platform, high-level accounts can get an overview of all files that are being transferred between systems. This helps to understand how files are being used and accessed, as well as ensure that files are arriving as expected at their destination. An MFT platform helps to consolidate and keep files more secure, enhances auditing and access history, and simplifies workflows.

### Consolidate and keep file transfers secure

One feature of MFTs is that they can regulate and consolidate transfer protocols. For example, SFTP is a secure way to transfer files. But some systems don't support SFTP and may require using another protocol like FTP instead. However, FTP is less secure, which is not ideal for sensitive file transfers. An MFT can force SFTP so that the files are sent in a more secure method, and do so across any system connected to the platform.

It's also a safer way to send files. An MFT can replace sending attachments via email, which is less secure and also vulnerable to spoofing. On top of this, some MFTs have antivirus software that scans attachments and won't transfer flagged malware between systems, let alone give users the chance to open the infected file.

### Enhance auditing and access history

When tracing file access is important to an organization, an MFT provides comprehensive reporting and access logs. Through these logs, admins can see who added or removed folders, when files were opened, and each individual login with a timestamp.

This can help in case of a data breach to trace the source, but it can also assist with restoring files that may have been altered unintentionally.

MFTs are also a safer way to transfer files. An MFT can replace sending attachments via email, which is less secure and also vulnerable to spoofing. On top of this, some MFTs have antivirus software that scans attachments and won't transfer flagged malware between systems, let alone give users the chance to open the infected file.

## Simplify workflows

Moving files through a centralized hub is useful, but the feature is much more useful when it can be done automatically. Many MFT platforms allow for this through file transfer automations. These automations can be set to trigger based on an action like a file being uploaded to a specific folder, or on a schedule like daily, weekly, or monthly.

Automations help financial institutions overcome the three obstacles outlined earlier as well. They are secure because only files that match set parameters are transferred, and the individual system doesn't require manual log-on. They increase accessibility by ensuring that required files end up precisely where they need to be at the right time, without the risk of omissions from a human operator. And they are reliable because they happen at the same time or when the specified action occurs immediately; some platforms such as Couchdrop will also inform users if an expected automation fails so it can be retried or the issue rectified by staff.

Automation use cases will be covered in more detail in a later section.

# Working with Legacy and Proprietary Systems

One of the biggest challenges for banks and financial institutions when it comes to file transfers is finding a system that integrates with software. It is not uncommon for financial institutions to use bespoke software or to have secure on-premises servers that generate files.

Many SFTP and MFT platforms have trouble reliably connecting to systems like these. But many financial institutions would rather find a reliable solution for securely transferring files rather than change to new software, which requires new onboarding, training, and protocol adjustments.

There are a few different solutions to move files between systems. MFTs are one way to do this while also gaining additional benefits provided through managed file transfers.

### How to connect an MFT to legacy or proprietary systems

Depending on the specific MFT you use, there are a few different ways to connect. Some require a custom API so that your bank software can communicate with the MFT.

With Couchdrop, the Windows/Mac Agent can be installed on any server running either of these operating systems. Files generated on that server can then be securely pushed through into Couchdrop via SFTP, and from there can be transferred to any other cloud storage connected such as Azure or Dropbox Business.

The agent is a low-resource program that can also run as a service. When combined with Couchdrop automations, it can send specific files generated on the server and automatically act on them, such as moving files from a certain folder into cloud storage daily.

For a simple setup guide with Couchdrop, see the article SFTP for banking and financial institutions.

# Couchdrop MFT for finance

Couchdrop is a cloud-native MFT that emphasizes privacy and security. Couchdrop's modern serverless architecture also allows for maintenance-free file transfers. These transfers are fast and effortless, and scale to meet user needs. A secure upload portal allows both staff and clients to securely upload files. Granular controls limit access on a per-user basis. And Couchdrop automations allow for intricate and complex setups compared to most MFTs.

### Couchdrop Security

Couchdrop takes security seriously and is always working to improve security for clients. It meets strict SOC2 compliance guidelines, which, according to the SOC2 website, "focuses on a business's non-financial reporting controls as they relate to Security, Availability, Processing integrity, Confidentiality, and Privacy."

Another way that Couchdrop reinforces data is by not storing data on its servers unless a customer chooses the hosted storage option. Couchdrop does not store data at rest or in transit, instead working as an intermediary to move files between a user's own cloud storage accounts. This key benefit of Couchdrop allows users to integrate their existing cloud storage and make a fluid connection between various storage platforms in Couchdrop's web interface.

### Maintenance-free file transfers

As a truly cloud-native MFT, Couchdrop allows for scalable, maintenance-free file transfers. There are no virtual machines to spin up or software to update. Couchdrop takes care of all the maintenance, and the modern architecture doesn't require system-wide downtime for updates.

This means there is no installing security patches or managing machines either. The infrastructure scales to meet the needs of each specific job, whether it is a single file transferred daily or thousands of files being relayed to hundreds of users.

## Fast file transfers

When files need to be accessed daily, it's important that the speed of the MFT platform is fast enough to move the files for further action. The same architecture that allows for maintenance-free file transfers also enables unrivaled file transfer speed.

This speed was fast enough that a second product, Movebot, was built off of the Couchdrop infrastructure and designed for large-scale transfers. Movebot can move 5TB or more per day between cloud platforms, uses the same architecture as Couchdrop, and is currently the only SOC2-compliant data migration tool available.

For smaller transfers, this means transfer speed is a non-issue. Couchdrop quickly moves files to the destination without hangups or waiting for required hardware. Using automations, regular transfers can also be automated for maximum accessibility.

## Secure Upload Portal

Couchdrop's Inboxes feature creates a secure upload portal that uploads files to a specified directory on the integrated cloud or on-prem storage. The white-labeled inbox can be customized with company branding and messaging, while still using Couchdrop's fast and secure infrastructure.

The secure upload portal has its own link that can be shared with clients or employees to quickly upload files. It can also be combined with a form, such as a registration form for customer details, which is a useful feature when supporting documents are required as part of registration for a particular service. The form entry will be connected to the attached document and further action can add details to an ERP or CRM system.

## Granular access control

To combat the three main reasons employees don't follow security protocols, Couchdrop includes granular access controls to remove unsecure options. When creating a user, a specific directory can act as their top-level directory.

Users can also be given restrictions on file actions, such as read-only, write-only, or read/write access. These can be granted account-wide or on a per-folder basis. Other access controls include allowing or denying access to Inboxes, specific transfer protocols like FTP, restricting to a specific IP address like an in-office workstation, and more.

As Couchdrop integrates directly with cloud storage, these access permissions can apply to directories used as a mount point for cloud storage as well. With Couchdrop's powerful access controls, users can have access only to what they need while still being able to work fluidly between platforms.

## Couchdrop Automations

With some of the most powerful automations available from any MFT, Couchdrop automations can significantly simplify file transfer workflows. Currently, there are 11 different actions, including PGP encryption and decryption for additional file security.

One standout feature of Couchdrop automations is the option to send a custom webhook. This can trigger a more advanced custom action configured in another platform, which in turn can simplify a multi-step workflow by not having to trigger the webhook manually.

Within Couchdrop, the platform supports multi-step automations that can both simplify processes and increase accuracy. For example, a data feed could save a file of daily transaction data to a specific folder on an on-prem server. An automation can copy that file into another storage platform such as SharePoint in a presentation folder. It could then rename that file using a timestamp. With this method, only the specific file originating in the original server directory would be renamed, as opposed to creating an automation for the presentation folder that would rename upon an upload and affect all files on upload. Instead of having to build separate small automations to work around this issue, it can all be done in a single multi-step automation within Couchdrop.

Automations, combined with Couchdrop's unmatched storage integration, means that users can automate file transfers for nearly any scenario. Since Couchdrop is able to connect to cloud storage as well as servers running Windows or OSX, and also run intricate, multi-step automations, time spent on file transfers can be significantly reduced throughout the organization.

## Additional Features

Couchdrop has a number of additional features that can benefit financial institutions and banks. Some of these include:

- Robust and comprehensive reporting including error logs and access reports.

- Fast and easy SFTP setup with no config files or virtual machine setup required.

- Shared links for individual files with options for expiration or password protection.

There are several other features and benefits of using Couchdrop in banking and finance. For more information see the platform overview page or email the support team at support@couchdrop.io.

# Conclusion

The banking and financial sectors require significant levels of security to protect sensitive and valuable information from falling into the wrong hands. Advances in technology have led to new ways of banking and digitizing files, and when handled properly, these industries can take advantage of the many benefits of cloud security.

However, these benefits also bring on new risks in cybersecurity. And although cyberattacks tend to be more covert and subtle compared to physical robberies, the losses to financial institutions and banks can be substantially more severe. Staying up to date with the latest security threats and ensuring software and systems stay updated with security patches and heightened protocols helps protect against data breaches.

One way to make use of cloud computing while following cybersecurity best practices is to use a reliable managed file transfer platform. MFTs reduce risk by acting as a central hub that all files flow through, allowing for updated security protocols and also tracking when and where files and directories are accessed and by whom. A dynamic MFT like Couchdrop also includes comprehensive file automations to simplify workflows and can connect to existing storage.

Couchdrop's modern serverless architecture never stores client data and simply facilitates file transfers between connected storage at high speeds so files quickly arrive where they need to be. This infrastructure also requires no maintenance or managing machines, and it scales automatically to meet the needs of each job. Granular access controls limit access to important or sensitive data, and powerful automations can move, copy, and protect files, along with the option to trigger a custom webhook for more advanced functionality.

MFTs are an excellent option for facilitating file transfers between different platforms. With no data storage, fast and comprehensive transfers, and a suite of helpful features, Couchdrop is an ideal MFT for use in the banking and financial sectors.

To find out more about how Couchdrop works or additional features about the product, contact Couchdrop support or email support@couchdrop.io.