SECLORE

FINANCIAL SERVICES BUSINESS USE CASES

FINANCIAL SERVICES

SECLORE

Protecting Agricultural Loan Verification Documents

Company Profile

Leading Financial Services Organization

- US$ 340 billion annual revenue
- 37,000+ employees
- 2220+ branches

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Outsource and Collaborate Securely
- Securely Adopt File-Sharing, Cloud, BYOD, and Mobile Device Usage
- Reduce Enterprise Risk and Liabilities
- Comply with Legal, Regulatory and Privacy Obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy, Edit, Print, and Screen Captures, by User, Time, and Location
- Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time – Wherever They Reside

It's not Just About Securing Information,
It's About Securing *Corporate Value*

Business Situation

The Financial Services company accepts written loan requests (for Retail Agricultural Loans) across many branches. The scanned copy of these loan requests (mortgaged property documents, KYC details, etc.) are shared with the respective Fraud Control Units (FCUs) stationed at the regional centers. The FCUs are responsible for obtaining Contact Point Verification (CPV) and Land Record Verification (LRV) from outsourced agencies. These agencies generally use printed copies of the documents sent to them by the FCUs for on-field verification of customer addresses, contact details, property verification from government offices, etc. The FCUs share a template with the verification agencies which is used for responding with verification reports and assessments.

Challenge

The branches share a scanned copy of the loan documents and KYC details with FCU team members stationed at the respective Regional Center. These documents can be in .pdf, .jpeg, .tif, .xls formats. They are emailed to the outsourced agencies by the regional centers.

This information is highly vulnerable to leakage by FCU team members and by employees of the vendor organization. It can also be leaked out over the communication channel or storage mechanisms – email, SFTP etc.

The challenge is to enable only authorized users to have only the required access rights (viewing, editing, printing etc. as required) on the confidential documents. Leakage of these documents may lead to business and reputational losses – not to mention a loss of market competitiveness.

Seclore Solution

All confidential data files are protected by the FCU team member using Seclore's Enterprise Digital Rights Management solution as soon as they are received from the branches. Only the authorized FCU team members have (restricted) access on the data files. This protection also travels with the file till it reaches the third-party agencies. Only authorized employees of the vendor organizations have the required access on the data files. Even if an unauthorized person gets hold of these files, he/she would not be able to open them.

The operations that each authorized person can perform on the file i.e. Viewing, Editing, Printing, Copying, etc., are also controlled. In fact, even the validity of the files can be defined and controlled, so they are automatically made unusable after their purpose is served. The Business unit power user, who is the owner of this information, can modify the Seclore protection and access permissions on these documents and can add/remove user access as desired. All the user activities are monitored and a searchable log of this information is available through a central web-based console.

Solution Delivered

The branches share the loan request documents with the FCU team at the respective regional centers.	
The data files are protected by the FCU team members using Seclore's EDRM Solution.	This ensures only authorized team members are able to access the data files and safeguarded the data files from leakage and misuse. Unauthorized users cannot access these files even if they obtain access to them.
These protected data files are then shared via email with the respective CPV and LRV agencies. A protected blank template is also shared.	Selected named employees of these agencies are permitted to view, print, and copy content from the document to the protected template – only for a period of 30 days. After this period, all documents expire and cannot be accessed by anyone in the agencies. This ensures that only the authorized agency employees can access and print the data files.
The agencies update the protected template with their feedback and status comments and send it back to the FCU team.	The process of editing and working on a protected file is virtually the same as that of working with a normal file. There is no change in user experience for authorized actions.
The documents sent to the agency expire after 30 days and cannot be opened by anyone.	This expiration occurs automatically. These files can also be expired manually before the 30-day period with a single click by the file owner(s) from the FCU team.

With Seclore's EDRM solution, the dependence on adherence to the contract signed with the agency – that states that all assets are supposed to be destroyed after a particular engagement/project is completed – is virtually eliminated. The legal agreement can actually be digitally enforced using Seclore's EDRM technology. Seclore has helped the financial organization ensure that information is secure and stays secure throughout its lifecycle – even when it is sent outside the company to outsourced agencies. With Seclore's EDRM, information security can be extended to areas outside the company's borders (to wherever the information travels) without affecting collaboration with third-parties. The financial services organization can now ensure that its customer information cannot be misused or leaked, and also comply with multiple regulatory and compliance mandates.

SECLORE

Protecting Information Sent to Collections Agencies

Company Profile

Leading Financial Services Organization

- US$ 340 billion annual revenue
- 37,000+ employees
- 2220+ branches

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Outsource and Collaborate Securely
- Securely Adopt File-Sharing, Cloud, BYOD, and Mobile Device Usage
- Reduce Enterprise Risk and Liabilities
- Comply with Legal, Regulatory and Privacy Obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy, Edit, Print, and Screen Captures, by User, Time, and Location Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time – Wherever They Reside

It's not Just About Securing Information,
It's About Securing Corporate Value

Business Situation

The Collections team is responsible for the collection of outstanding amounts from the company's delinquent customers for secured and unsecured loans, Agricultural loans and Credit Cards. The IT team extracts the relevant data from the enterprise system and shares data files of delinquent accounts with the Collections team.

The Collections team then outsources the work to third party Collection agencies, based on location and category. Sensitive customer information is shared with these agencies via email. Each Collection agency assigns Feet on Street (FOS) agents to delinquent accounts for collection and follow up. The Collection Agency then collates the feedback for each outstanding account and emails the Daily Collections Report to the financial institution's Collections team for tracking.

Challenge

Collections team (internal) and the Collection agencies (external) have access to financially sensitive and confidential PII (Personally Identifiable Information) which is very valuable to the organization. These data files are vulnerable to leakage by any Collections team member or by any employee possessing access to the shared folder where the files are stored. This data is also vulnerable to leakage while it is transferred over the communication channel – email, FTP, etc. It is also exposed to leakage and theft in the offices of the Collections agencies – that may not possess a rigid security infrastructure and IT systems.

Loss of this information could lead to significant financial and business losses to the company. It could also result in negative press coverage and a loss in consumer confidence. Moreover, regulatory and statutory obligations mandate financial institutions to encrypt and ensure the safety of sensitive customer data – both within and outside the company.

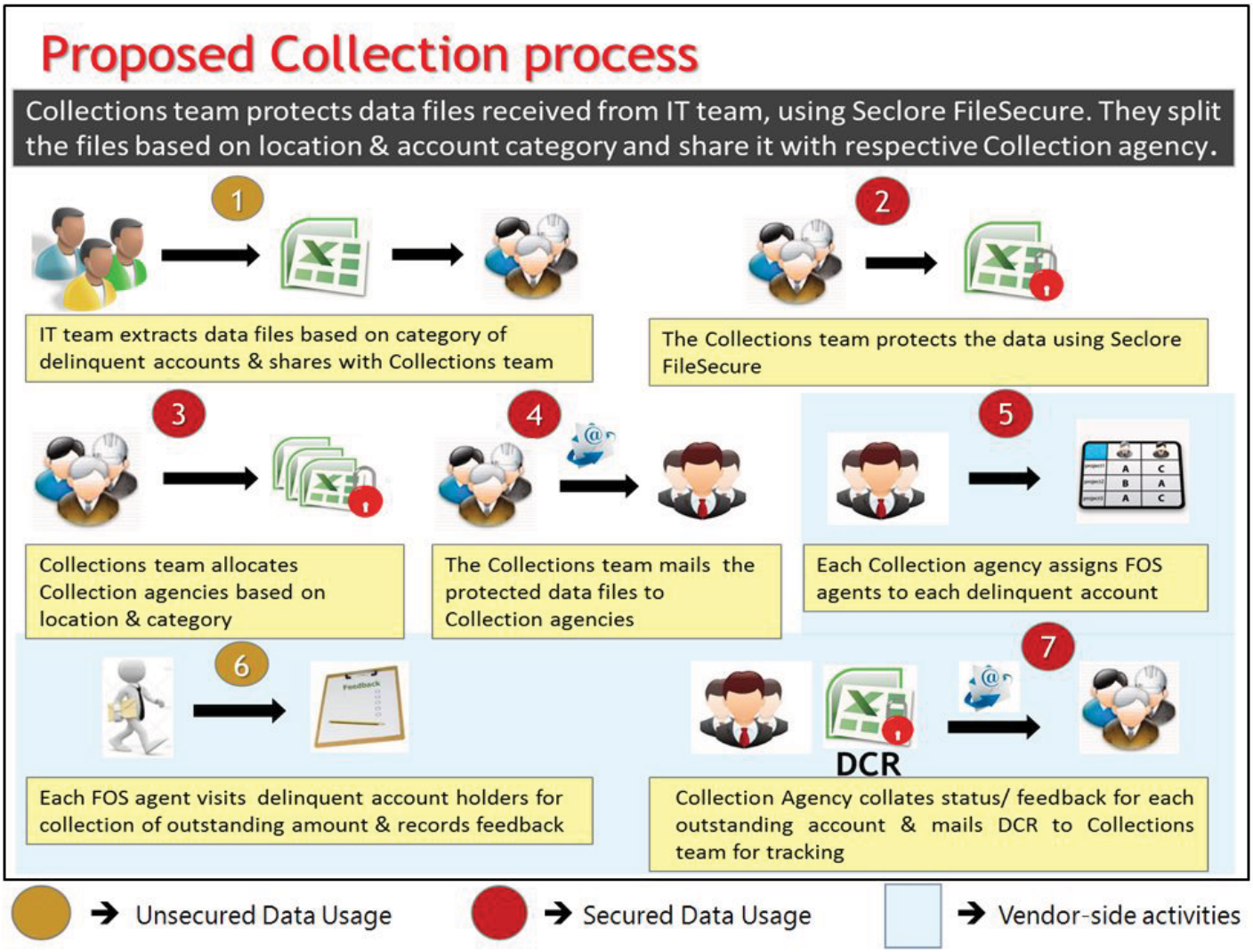
The challenges this situation presents are:

1. To enable only authorized business users to access these confidential documents
2. To restrict the activities of authorized users as well, e.g. users authorized to view a document should not be able to print it or copy its contents to another file or email
3. To comply with regulatory guidelines and compliance mandates.

Seclore Solution

All confidential data files are protected using Seclore's EDRM by the Collections team after receiving it from the IT team. Only the authorized Collections team members and zonal managers possess the required access on their respective files. This protection sticks to the file and is equally effective in the Collections agencies' environments. Only authorized users at each agency have permissions to access these files. Any other user cannot open these files even if he/she gets hold of them.

The operations that each authorized person can perform on the file i.e. Viewing, Editing, Printing, Copying, etc., are also controlled and monitored. Audit reports of activities performed on each file are available from a central web-based console. Even the validity and expiry date of each file can be defined, so that they are automatically made unusable after their purpose is served. This ensures the fulfilment of an important contractual obligation and reduces the dependency of data security on just a piece of paper.



Solution Delivered

The data files received from the IT team are protected by the Collections team.	This is a simple process that involves dipping these files into a special Windows folder and then taking them out. Multiple files can be protected simultaneously in one go.
Zonal Collection managers are provided permissions to view, edit and copy content out of the files. This enables them to easily create multiple data files according to location and account category, and assign these to the respective collections agencies.	This ensures that only authorized Collections team members and the relevant zonal managers are able to access this information. Customer information is thus safe from theft and misuse.
These protected files are then shared with the respective Collections agencies via email. Designated users at these agencies possess permissions to view, edit and print the files – all only for a period of 30 days.	This ensures that only the authorized agency users can access the data files and take printed copies for field verification (Feet On Street) agents.
The data files are then edited by the agencies with the feedback/status and sent back to the Collections team of the financial company	There is no change in the user experience of editing a protected file from that of editing an unprotected (normal) file. Existing processes and workflows do not get affected in any way with the introduction of Seclore's EDRM.

The above solution ensures end-to-end protection of confidential customer data being sent to third party collection agencies. Hence, security – which is traditionally seen as a hindrance to external collaboration – has now become a business enabler. Seclore's EDRM solution has helped the organization to safely and securely outsource collections activities to as many external agencies as needed while increasing focus on its core competencies. This leads to increased efficiency, increased productivity, and increased business output. The financial services company has not only mitigated the risk of data theft and leakage, but has also met regulatory and compliance obligations. The financial organization has not only successfully secured its information, but has also secured its business and reputation.

About Seclore

Seclore offers the market's first fully browser-based data-centric security solution, which enables organizations to control the usage of files wherever they go, both within and outside of the organization's boundaries. The ability to remotely enforce and audit who can view, edit, copy, screen share, and redistribute files empowers organizations to embrace mobility, file-sharing, and external collaboration with confidence. With over 2000 companies in 29 countries using Seclore to protect 10 petabytes of data, Seclore is helping organizations achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.
Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

USA – West Coast
691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

India
Excom House Second Floor
Plot No. 7 & 8
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Gurugram
+91 124 475 0600

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 7621 5500 350

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

SECLORE