PROTECTING CLIENT DATA IN BANKING COMMUNICATIONS

SafeSuite Lite provides secure email communication that reinforces client trust and banking governance.

Email Risk for Banks

Banks are entrusted with their clients' most sensitive financial information. Every day, that data is shared over email, including loan documents, account statements, and identity files. A mis-send or forwarded attachment can create significant regulatory and reputational risk. SafeSuite Lite helps banks protect nonpublic personal information (NPI) at the file level, maintaining control, encryption, and audit visibility even after documents are shared.

A Practical Approach

SafeSuite Lite works directly within existing email workflows, allowing bankers to protect sensitive documents when they are sent, supporting banking privacy and safeguard requirements. Protection and access rules are embedded into each file, so security travels with the document wherever it goes. Banks can continue communicating with clients via email without losing control after delivery, while maintaining peace of mind for clients.

How It Works

Banker emails documents as usual
Email messages and attachments are protected and sent as secure links.

Client opens securely
No new accounts, logins, or portal. A one-time passcode verifies access.

Bank stays in control
Access is tracked, policies can be updated, and files can be revoked anytime.

Use Cases

- Loan and Mortgage Documents
- Account Statements and Disclosures
- Client Notices and Correspondence
- Identity and Onboarding Forms
- Advisor and Third-Party Files
- Regulatory and Audit Materials

Colorado
keyavi.com
info@keyavi.com

Built for Bankers and Clients

No New Portals
Clients access documents through a secure link. No accounts or portals required.

Governance Ready
Supports requirements, including GLBA-aligned data protection and audit visibility.

No Workflow Changes
Bankers protect files directly from Outlook or Gmail without changing how they work.

Familiar Security
Clients verify access with a one-time passcode, aligning with standard banking processes.

Case Study

Situation

A regional bank regularly shared sensitive financial documents with clients via email. While email was convenient, clients wanted clear reassurance that their personal and financial data was protected. Internally, the bank lacked visibility once files were sent, creating concern around regulatory exposure and meeting GLBA-aligned data protection expectations.

Solution

The bank selected SafeSuite Lite to give clients confidence that their data was protected, without introducing complex portals or disrupting familiar email communication. By securing documents at the file level, the bank could maintain oversight and control while providing clients with a simple, trusted way to access their information.

Results

- Increased client confidence that their data was protected.
- Secure, compliant email communication without workflow disruption.
- Improved governance confidence with GLBA-aligned audit visibility.
- Reduced risk from mis-sent or forwarded documents.
- Improved trust in digital client interactions.

Client trust starts with data control. Discover how SafeSuite Lite secures client data in everyday banking. Contact info@keyavi.com for a demo.