DISCLAIMER: *infotex is not a law firm, and does not staff attorneys.*

Executive Summary: Email Retention for Community Banks

Email retention is a critical topic for community banks, but the legal landscape surrounding it remains unsettled. Various agencies and entities have published guidelines and requirements, leading to a complex regulatory environment. This summary aims to provide an overview of email retention guidance from federal regulators, as well as a summary of relevant state laws for Indiana and Ohio. To navigate these challenges effectively, it is recommended to incorporate appropriate policies, reviewed by legal counsel, that address email retention practices specific to each institution.

Contents:
To help you understand the landscape, this white paper includes the following details:

- **Federal Regulators:**
  The FFIEC and different federal regulators provide vague guidance on email retention for community banks. We have included a guidance review below.

- **Memo from (the infotex attorney):**
  Indiana and Ohio state laws can also impact email retention requirements. We asked our attorney to speak to this in a memo, which (with his approval) is attached in a separate pdf.

Recommended Approach:
Given the complex and disparate laws and regulations, coupled with the challenge of keeping track of them, we recommend you consult legal counsel.

It may be helpful to develop a comprehensive email retention policy prior to that consultation. Our attorney recommends using a seven-year retention period, given that seven years is the longest of all the disparate retention requirements.

Date: 06/08/23

DISCLAIMER: *While we attempt to assert that this document includes all information available on the various agency websites as of the date listed above, we offer this as an aid to audit and consulting Clients, and in no way warrant this as being all-inclusive, complete, or thorough. Please use at your own risk.*

GLBA

Under the Gramm-Leach-Bliley Act (GLBA), there are no specific email retention requirements outlined. GLBA is a United States federal law that governs the privacy and security of customers' personal financial information held by financial institutions. While GLBA does not explicitly address email retention, it does require financial institutions, including banks, to implement safeguards to protect the confidentiality and integrity of customer information. These safeguards include:

Privacy Policy: Banks must have a privacy policy in place that outlines how they collect, use, and disclose customer information.

Information Security Program: Banks must develop and maintain an information security program that protects customer information from unauthorized access, use, or disclosure.

Safeguards Rule: The Safeguards Rule under GLBA requires banks to implement measures to ensure the security and confidentiality of customer information. While it doesn't specify email retention, it emphasizes the importance of protecting customer data throughout its lifecycle, including during storage, transmission, and disposal.

While GLBA does not provide specific guidance on email retention, other regulations and industry best practices may apply. Additionally, state laws and regulations may impose specific requirements for email retention, particularly concerning financial institutions operating within those states. It's important for banks to consult legal counsel and industry experts to ensure compliance with all relevant laws and regulations regarding email retention and data security.

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) does not establish specific email retention requirements, it provides guidance on recordkeeping practices for financial institutions, including banks. According to the FFIEC, banks should establish and maintain comprehensive records management programs that cover all types of records, including electronic records such as emails.

The guidance encourages banks to develop policies and procedures for the retention and disposal of records, including emails, based on legal and regulatory requirements, business needs, and industry standards. The FFIEC suggests that banks consider the following factors when determining email retention periods:

Legal and Regulatory Requirements: Banks should be aware of any specific legal or regulatory requirements that apply to their operations. Certain laws or regulations may mandate minimum retention periods for certain types of records, including emails. It's crucial for banks to stay informed about the applicable laws and regulations within their jurisdiction.

Business Needs and Operational Requirements: Banks should consider their specific business needs and operational requirements when establishing email retention periods. These considerations may include the need for quick access to records, potential litigation or regulatory investigations, and industry best practices.

Risk Management: Banks should assess the risks associated with email retention, including the potential for unauthorized access, data breaches, and compliance violations. Risk assessments can help banks determine appropriate retention periods and implement necessary safeguards to protect sensitive information.

FDIC

The Federal Deposit Insurance Corporation (FDIC) does not have specific email retention requirements but offers guidance on recordkeeping practices that can be applied to emails. The FDIC encourages banks to establish and maintain comprehensive recordkeeping programs that encompass all types of records, including electronic records such as emails. Banks should develop policies and procedures for the retention, retrieval, and disposal of records based on legal and regulatory requirements, business needs, and industry standards.

While the FDIC does not outline specific email retention periods, it suggests that banks consider the following factors when determining retention periods for emails:

Legal and Regulatory Requirements: Banks should be aware of any legal and regulatory requirements that dictate record retention periods. Specific regulations may stipulate minimum retention periods for certain types of records, and banks should comply with these requirements. It is essential to stay informed about the relevant laws and regulations that apply to the bank's operations.

Business Needs and Operational Requirements: Banks should assess their business needs and operational requirements to determine appropriate email retention periods. Factors to consider include the need for quick access to records, potential litigation or regulatory inquiries, and industry best practices.

Risk Management: Banks should conduct risk assessments to identify and manage the risks associated with email retention. This includes risks such as unauthorized access, data breaches, and non-compliance with legal and regulatory obligations. Risk assessments can help banks determine suitable retention periods and implement necessary safeguards to protect sensitive information.

FEDERAL RESERVE

The Board of Governors of the Federal Reserve System (the Fed) does not provide specific email retention requirements for banks. However, it offers guidance on recordkeeping practices that can be applied to emails.

The Fed encourages banks to establish comprehensive recordkeeping programs that cover all types of records, including electronic records like emails. Banks are expected to develop policies and procedures for the retention, retrieval, and disposal of records based on legal and regulatory requirements, business needs, and industry best practices.

While the Fed does not outline specific email retention periods, it suggests that banks consider the following factors when determining retention periods for emails:

Legal and Regulatory Requirements: Banks should be aware of any legal and regulatory requirements that govern record retention. Specific regulations may impose minimum retention periods for certain types of

records, and banks should comply with these requirements. It is crucial to stay informed about the relevant laws and regulations that apply to the bank's operations.

Business Needs and Operational Requirements: Banks should assess their business needs and operational requirements to determine appropriate email retention periods. Factors to consider include the need for quick access to records, potential litigation or regulatory inquiries, and industry best practices.

Risk Management: Banks should conduct risk assessments to identify and manage the risks associated with email retention. This includes risks such as unauthorized access, data breaches, and non-compliance with legal and regulatory obligations. Risk assessments can help banks determine suitable retention periods and implement necessary safeguards to protect sensitive information.

OCC

The Office of the Comptroller of the Currency (OCC) provides guidance to banks regarding various operational aspects, including recordkeeping practices. While the OCC does not specify email retention requirements, it offers guidance on record retention that can be applied to emails.

According to the OCC's guidance on recordkeeping, banks are expected to establish and maintain comprehensive recordkeeping programs that encompass all types of records, including electronic records like emails. Banks are encouraged to develop policies and procedures that address the retention, retrieval, and disposal of records, taking into consideration legal and regulatory requirements, business needs, and industry standards. When determining email retention periods, the OCC suggests that banks consider the following factors:

Legal and Regulatory Requirements: Banks should be aware of applicable laws and regulations governing record retention. Specific regulations may impose minimum retention periods for certain types of records, and banks should comply with these requirements. It is important to stay informed about the relevant laws and regulations that apply to the bank's operations.

Business Needs and Operational Requirements: Banks should assess their business needs and operational requirements to determine appropriate email retention periods. Considerations may include the need for quick access to records, potential litigation or regulatory inquiries, and industry best practices.

Risk Management: Banks should conduct risk assessments to identify and manage the risks associated with email retention. This includes potential risks such as unauthorized access, data breaches, and non-compliance with legal and regulatory obligations. Risk assessments can help banks determine appropriate retention periods and implement necessary safeguards to protect sensitive information.

E-Sign

The Electronic Signatures in Global and National Commerce Act (E-Sign Act) is a United States federal law that establishes the legal validity and enforceability of electronic signatures and electronic records in interstate and foreign commerce. The E-Sign Act itself does not specifically address email retention requirements for banks or any other entity. However, the E-Sign Act does recognize the legal validity of electronic records, which can include emails.

It states that electronic records, including emails, may satisfy legal requirements if they are accurately preserved and can be accessed in a manner that is both accurate and accessible for later reference. While the E-Sign Act

does not provide specific guidance on email retention periods, it emphasizes the importance of maintaining the integrity and accessibility of electronic records, including emails. Banks, like any other organization, are responsible for establishing their own policies and procedures for the retention and management of electronic records, including emails, in compliance with applicable laws and regulations.

While these entities guidance's provide a framework for banks to develop their own email retention policies based on their specific circumstances. Banks should consult legal counsel, compliance professionals, and refer to other applicable regulatory guidelines to ensure their email retention practices are in line with the requirements and expectations and other relevant authorities.