KPMG

# Regulatory Alert

**Regulatory Insights**

**April 2024**

## Data Retention and Deletion: Devices and E-Comms

***KPMG Insights:***

- ***Scrutiny on Unauthorized Communications:*** *Enforcement trends highlight the critical need for firms to capture and retain all business-related communications, including those on personal devices.*
- ***Expanding Scope of Data:*** *The types of data subject to regulatory expectations for retention and deletion continues to expand as technologies evolve.*
- ***Tighter Data Controls:*** *Increasing regulatory actions demand stringent protection of customer data; retention and deletion practices should emphasize data minimization, purpose limitation, and enhanced privacy compliance.*

---

Regulators continue to focus heightened attention and enforcement on data, including issues related to data/records retention. This focus includes:

- Data retention associated with maintaining and preserving business communications conducted through unauthorized, "off-channel", communication methods.
- Data protection safeguards, including the introduction of new laws and rule updates (at the state and federal levels) limiting the amount of data that companies collect and retain, and for how long.

### "Off-Channel" Comms and Data Retention

Regulators continue to scrutinize and enforce against data retention/recordkeeping requirements for electronic communications. The focus is directed toward capturing and preserving business-related communications (both internal and external, in written and recorded forms) conducted through employees' use of personal devices (e.g., cell phones, tablets) or through "off-channel" communications methods (e.g., communications platforms, messaging applications, and social media websites not authorized for use by the employer whether on personal or company-provided devices). Notably, regulators' expectations for what comprises electronic communications continues to expand as technologies evolve.

Recent enforcement actions and related guidance reflect a focus on records retention, business conduct, and supervision requirements.

| Agency | Action |
|---|---|
| **SEC** | The Securities and Exchange Commission (SEC) charged and settled with dozens of supervised entities, including broker-dealers, investment advisers, and credit rating agencies, for failure to maintain and preserve off-channel electronic communications, and to reasonably supervise.<br><br>*(Note: In October 2023, SEC Director of the Division of Enforcement stated that the agency had charged 40 entities and assessed more than $1.5 billion in civil money penalties for failure to* |

| | |
|---|---|
| | *maintain and preserve electronic communications. Additional enforcement actions have been initiated since that time.)* |
| **CFTC** | The Commodity Futures Trading Commission (CFTC) issued numerous orders filing and settling charges with a variety of supervised entities, including introducing brokers, swap dealers, futures commission merchants, and affiliates of financial institutions for failing to maintain, preserve, or produce required records of communications via unapproved methods and to "diligently" supervise.<br><br>*(Note: In March 2024, the CFTC stated that the agency had charged 22 entities and assessed more than $1.1 billion in civil money penalties for the use of unapproved communication methods.)* |
| **DOJ** | As part of a legal action, the Department of Justice (DOJ) sought a decision from a U.S. District Court to sanction a defendant for failing to preserve "chat messages" potentially relevant to the litigation. |
| **DOJ, FINRA** | Guidance from the DOJ and the Financial Institution Regulatory Authority (FINRA) denote additional communication methods as subject to existing recordkeeping requirements, such as:<br><br>— Collaborative capabilities in third-party platforms (e.g., whiteboards, screen-sharing tools, and video and group chats).<br><br>— The use of emojis or other means to convey subtextual messages.<br><br>— "Ephemeral" messaging applications (i.e., where conversation histories disappear quickly either by design or at the user's option). |

## Potential Remedial Actions

The table below outlines remedial actions cited in recent regulatory enforcement orders.

| Topic | Action |
|---|---|
| **Independent Compliance Consultant** | Retain an independent compliance consultant to conduct a comprehensive review of company policies, procedures, and programs, focusing on the preservation of electronic communications, including those found on personal devices and to provide a detailed report and recommendations. The review may include:<br><br>— Supervisory, compliance, and other policies and procedures.<br><br>— Training for, and certification of compliance by, personnel.<br><br>— Assessing surveillance program measures, including communications surveillance routines to ensure compliance.<br><br>— Assessing technological solutions implemented to meet record retention requirements.<br><br>— Assessing measures used to prevent use of unauthorized communication methods by employees.<br><br>The consultant maybe also be retained to assess the company's progress toward preserving electronic communications, including complying with laws and regulations as appropriate, and to submit a progress report with an updated assessment of the company's policies, procedures, and technological efforts.<br><br>Under the enforcement actions, companies were required to adopt all recommendations in the consultant's report and to cooperate fully (e.g., provide access to files, books, records, and personnel, as needed). |
| **Notifications** | Notify the company's primary regulator of any discipline imposed on employees who have violated record-keeping policies. The regulators strongly encourage self-reporting and cooperation. |
| **Internal Audit** | Require Internal Audit to conduct an audit (separate from the compliance consultant review) to assess progress in the areas described above and submit a report to the company and regulator's staff. |

| | |
|---|---|
| **Related Recordkeeping** | Preserve records of compliance with these remedial efforts for an ongoing period. |
| **Certification** | Under the enforcement actions, companies were required to certify compliance with prescribed remedial efforts and to submit the certification along with supporting evidence to the regulator within a specified timeframe of completion. |

## Data Retention/Deletion Safeguards

Regulators have demonstrated an ongoing, keen focus on ensuring companies have sufficient safeguards for customer data, as well as appropriate retention and deletion practices. Select examples of regulatory actions in these areas are highlighted in the table below:

| Agency | Topic | Action |
|---|---|---|
| **FTC** | **Commercial Surveillance & Data Security** | The Federal Trade Commission (FTC) published an advanced notice of proposed rulemaking (ANPR) seeking public comment on commercial surveillance and data security practices, including those that relate to the FTC's Safeguards Rule. Among other things, the ANPR posed multiple questions on the collection, use, and retention of consumer data, including whether:<br>— Companies should be limited to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that an individual consumer explicitly seeks or those that are compatible with that specific service.<br>— New trade regulation rules should be imposed to restrict the period of time that companies collect or retain consumer data, irrespective of the different purposes to which it uses that data.<br>— Companies should be required to certify that their commercial surveillance practices meet clear standards concerning collection, use, retention, transfer, or monetization of consumer data. |
| | **Safeguards Rule** | The FTC published its final Standards for Safeguarding Customer Information (Safeguards Rule), applicable to financial institutions under the FTC's jurisdiction. The rule states that covered financial institutions must:<br>— Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two (2) years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is stores and managed.<br>— Periodically review their data retention policy to minimize the unnecessary retention of data. |
| **SEC** | **Regulation S-P: Safeguards & Disposal Rules** | The SEC settled charges against a large broker-dealer and investment adviser for alleged failures to protect customers' PII in connection with the disposal of decommissioned devices and other information technology assets that contained customer data, including PII.<br>— In particular, the SEC found the firm violated both its Safeguards Rule and Disposal Rule under Regulation S-P, which require, respectively, "written policies and procedures to address administrative, technical, and physical safeguards reasonably designed for the protection of customer records and |

| | | |
|---|---|---|
| | | information," and, at the time of their disposal, reasonable measures to protect against unauthorized access to, or use of, the data. |
| **State: CA** | **CPRA** | The California Privacy Rights Act (CPRA) became effective in 2023, establishing limitations on data collection and retention. More specifically:<br>— A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate (data minimization) to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes (purpose limitation).<br>— A business shall not retain a consumer's personal information or sensitive personal information… longer than is reasonably necessary for that disclosed purpose. |

**For more information** about data and records retention, please contact Steve Stein or Mike Sullivan.

## Contact the author:

**Amy Matsuo**
**Principal and National Leader**
Regulatory Insights
amatsuo@kpmg.com