**ORX News reference:** 12585
**ORX Standard:** Banking

| | |
|---|---|
| United States Department of the Treasury | USD Not Identifiable Loss \| US Dollar |
| USD Not Identifiable Loss \| US Dollar | EUR Not Identifiable Loss \| Euro |
| BL1001 - Corporate Items | EL0202 - System Security External - Wilful Damage |
| US - United States | North America |
| Loss Event | Published in media 08 April 2025 |

# OCC suffers email hack accessing sensitive information on financial institutions

On 8 April 2025, the US Office of the Comptroller of the Currency (OCC) released a statement saying it had informed Congress of “a major information security incident” in which hackers had accessed executives’ and employees’ emails which included “highly sensitive information” about financial institutions.

On 11 February 2025, the OCC detected unusual interactions between an administrative account in its email system and OCC user mailboxes. On 12 February 2025, the OCC confirmed that the activity was unauthorised and activated its incident response protocol, including initiating an external incident assessment and reporting the incident to the US Cybersecurity and Infrastructure Security Agency.

The OCC disabled the compromised administrative accounts and, in a public notice of the incident on 26 February 2025, confirmed that it had terminated the unauthorised access. In that statement, the OCC said its investigation had analysed all email logs since 2022 and that there was no indication of any impact to the financial sector.

Subsequently, however, the OCC carried out internal and independent third-party reviews which revealed that the information accessed via the email accounts related to the financial condition of federally regulated financial institutions. According to bloomberglaw.com, the OCC said in a letter to Congress that the hackers intercepted over 100 bank regulators’ accounts and accessed approximately 150,000 emails since May 2023.

The statement released on 8 April 2025 did not disclose specific weaknesses that led to the hack, but the acting Comptroller of the Currency, Rodney E. Hood, stated that “long-held organisational structural deficiencies” contributed to the incident.

The OCC said it was using third-party cybersecurity experts for the ongoing investigation. As of 8 April 2025, the OCC was launching an evaluation of its current IT security policies and procedures in order for it to better prevent, detect and remediate potential security incidents.

**Author:** Isabel Fernández **Published Date:** 09 April 2025 **Last Update:** 11 April 2025

| Published In Media | Occurrence - From | Occurrence - To | Discovery Date | Recognition / Settlement |
|---|---|---|---|---|
| 08 April 2025 | | 12 February 2025 | 11 February 2025 | |

| ORX Reference Taxonomy<br>RT1303 - Cyber events | | |
|---|---|---|
| **Boundary Risk**<br>Other Risk | **Industry Event** | **Scenario**<br>SC0023 - Cyber-Related Data Breach |
| **Product**<br>PD9900 - Not Product-Related | **Process**<br>PC1004 - IT Security | **Event Closed**<br>No |
| **ORX Member**<br>No | **Role of Firm**<br>LS0307 - Position Taking (Principal) | **Jurisdiction / Choice of Law**<br>LS0101 - United States of America |
| **Cause 1**<br>CS0102 - Assault by Criminals / Terrorists | **Cause 2**<br>CS0304 - Organisational Controls | **Cause 3**<br>CS0503 - Software - Inadequate Maintenance |
| **Counterparty**<br>LS0212 - Not Identifiable | **Environmental Volatility**<br>LS0406 - Not Identifiable | **Provision**<br>No |

## Source(s)

**https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html**
**https://www.law360.com/articles/2322803/occ-says-highly-sensitive-bank-info-accessed-in-hack**
**https://www.reuters.com/technology/cybersecurity/us-regulator-occ-notifies-congress-major-security-breach-2025-04-08/**
**https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-13.html**
**https://news.bloomberglaw.com/banking-law/hackers-spied-on-100-bank-regulators-emails-for-over-a-year**
**https://www.securityweek.com/treasurys-occ-says-hackers-had-access-to-150000-emails/**

## Related links