

Monthly Cyber Briefing

April 3, 2025



Meeting Logistics



Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A box.



Resources

Upcoming events, slides & resources linked.



Recording

Recording will be provided after event.



Survey

Survey will prompt at the end of webinar.

Agenda

- Cyber & Regulatory Update
- Lessons From the Field: Cybersecurity Trends Across the Healthcare Ecosystem
- Q+A



**Steve Cagle, MBA,
HCISPP, CHISL, CDH-E**

Chief Executive Officer
Clearwater

Cyber & Regulatory Update

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

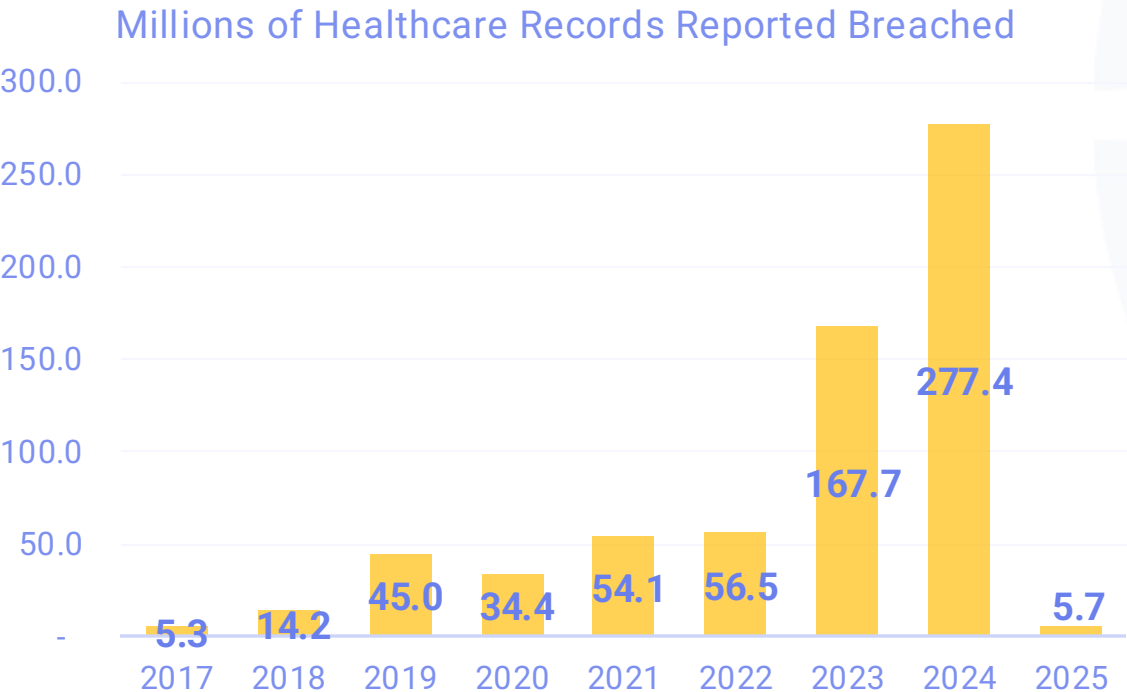
CEO, Clearwater



Breach Reports via OCR Breach Portal

OCR Breach Portal Data¹

- 2024 breach data: OCR updated to 277.4M records from 734 breaches
- YTD 2025 breach data: 5.7M individuals reported from 151 breaches, with 57 more than last Cyber Briefing



- Change Healthcare has now reported additional 90m records to previous 100m (total 190M)
- Additional 1.65M records updated from other breaches including 5 new reported in 2024
- Largest breach reported last 30 days was United Seating and Mobility, LLC d/b/a Numotion (494K individuals), which previously had a ransomware attack in 2024

¹ The [HHS Breach Portal](#) (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 2/24/25 pulled 3/30/25)

Alleged Oracle Cloud Infrastructure (OCI) Breach

Claimed hack of ~6 million lines of data from Oracle Cloud's SSO and LDAP.

Oracle customers confirm data stolen in alleged cloud breach is valid

By **Lawrence Abrams**

March 26, 2025 04:20 PM 10

Oracle cloud traditional hacked (login.(X).oraclecloud.com)
by rose87168 - Thursday March 20, 2025 at 02:40 PM

Yesterday, 02:40 PM (This post was last modified: Yesterday, 02:44 PM by rose87168.) #1

Hello,
Oracle traditional servers were hacked (domains : login.(region-name).oraclecloud.com)
Around 6 million user customers' data from SSO and LDAP was stolen.
JKS files, passwords, key files, and enterprise manager JPS keys were also taken.
The SSO passwords are encrypted, they can be decrypted with the available files. also LDAP hashed password can be cracked. (I couldn't do it, but if someone can tell me how to decrypt them, i can give them some of the data as a gift.)
I'll list the domains of all the companies in this leak. Companies can pay a specific amount to remove their employees' information from the list before it's sold.
i can also trade for 0-day exploits. send me a private message (PM).
oracle can send me a message through the company's official email to My Email with 72H (we talk before)

Sample LDAP >
Company list >
Sample DataBase >

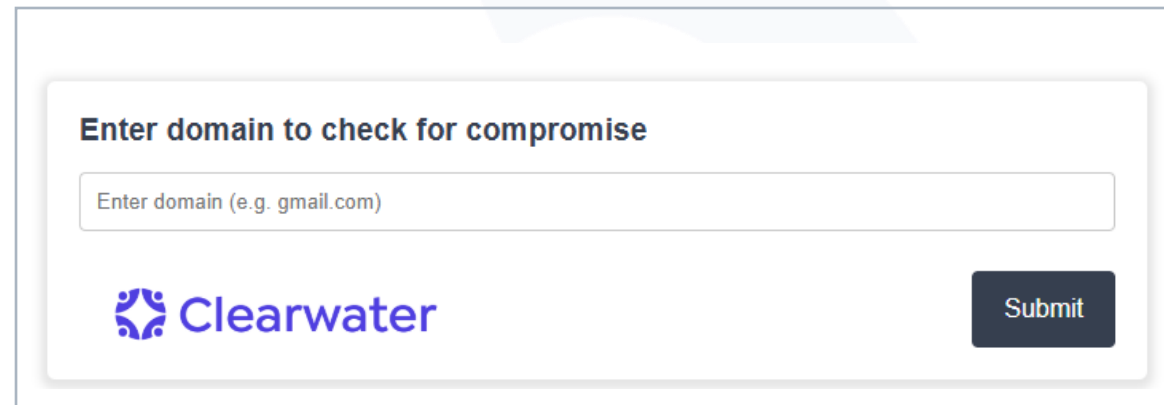
PM for Offer

- If cracked, stolen encrypted SSO and LDAP passwords could enable further Oracle Cloud breaches
- Hack supposedly includes JKS files, encrypted SSO passwords, key files, and enterprise manager JPS keys
- The threat actor claimed to have compromised the subdomain login.us2.oraclecloud
- Research firms validated Oracle fusion middleware had a critical vulnerability CVE-2021-35587
- TA provided evidence of write access to server, provided sample data, and published list of affected Oracle clients
- Oracle initially denied the claim and is now silent
- There are claims that Oracle is scrubbing evidence of the attack


Recommendations: Oracle “Classic” Cloud Breach

- Rotate any passwords or secrets that are shared amongst different services
- Update all SSO and LDAP integrations with new passwords, and consider continuing to rotate passwords
- Make sure to enable MFA to access all Oracle Cloud Apps
- A conservative approach would be to consider all Oracle Cloud services could to be potentially compromised
- Speak to your vendors that use Oracle Cloud and understand what steps they have taken to mitigate risks. updated as changes to your environment occur

[Click here](#) for
Clearwater’s Oracle
Breach Search web
page



Enter domain to check for compromise

 Clearwater

Submit

Oracle (Cerner) ePHI Data Breach

Some Oracle Health (Cerner) customers have received notification letters advising of a breach of ePHI

- Breach occurred on or after January 22, but discovered on February 20 on legacy Cerner data migration servers; resulted in impermissible disclosures of ePHI
- Oracle Health provided notification to customers on non-letterhead and requested all correspondence to CISO by phone and not in writing
- Oracle Health is allegedly telling hospitals that they will not notify patients directly
- It's been reported that hospitals are being extorted for millions of dollars
- Oracle's lack of transparency is being criticized

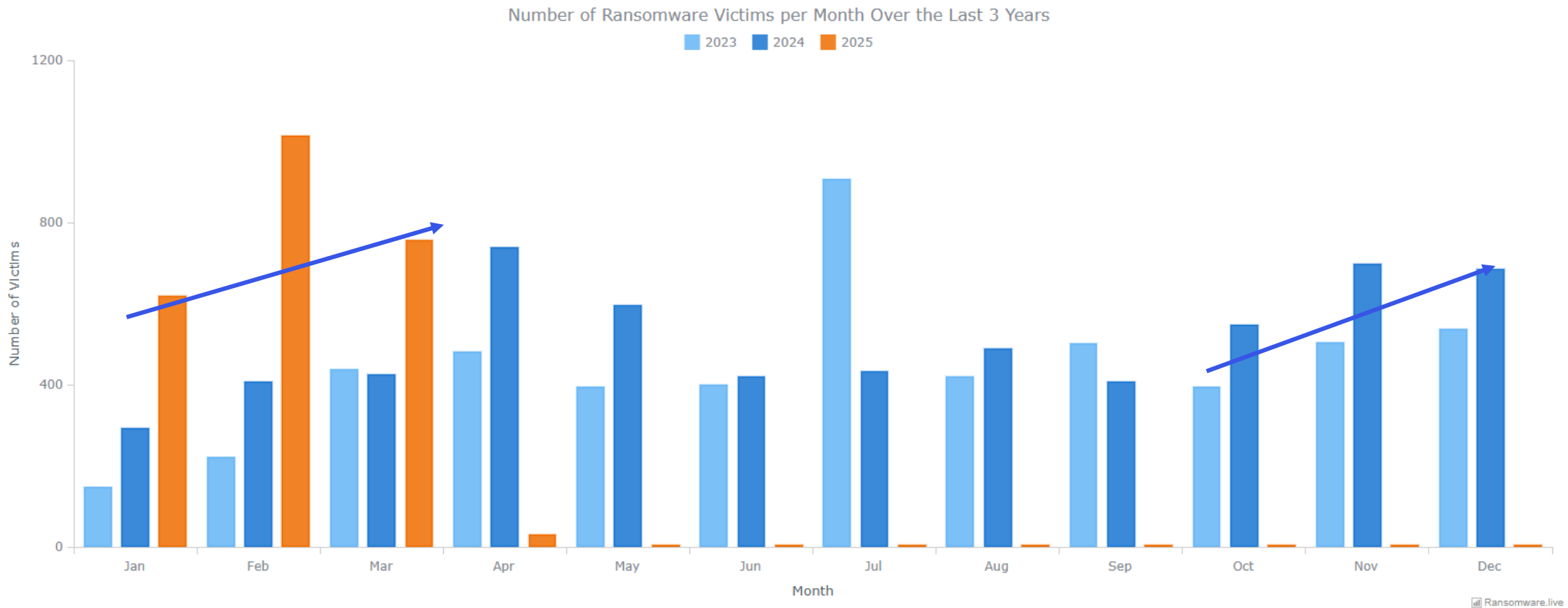


Recommendations

- Contact your Oracle Health representative if you are concerned about their breach
- If your organization is involved in the breach, consult your business associate agreement and activate IRPs

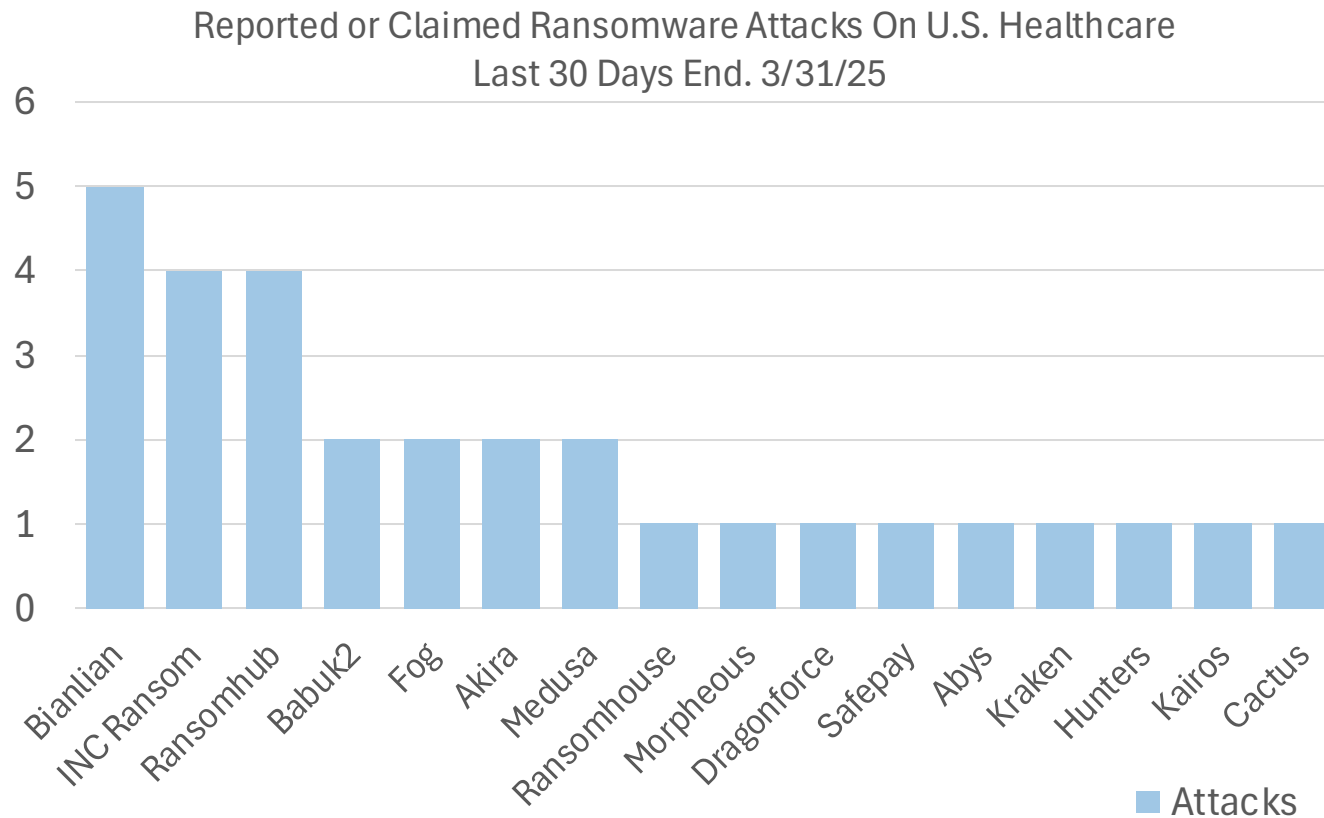
Ransomware Attacks Increasing Globally

2,388 claimed or reported ransomware attacks across all industries globally in first three months of 2025 vs 1,122 in 2024. Continued trend of increased attacks, which began in Q4 2024.



Ransomware Attacks on Healthcare Last 30 Days

34 identified attacks on U.S. Healthcare organizations 2/16/25 – 3/31/25



- Healthcare sector continues to be highly targeted
- BianLian, IncRansom and RansomHub remain top threat actors targeting healthcare
- New ransomware threat actors are entering market
- Notable attacks:
 - Loretto Hospital in Chicago discovered attack March 10. Both IncRansom and RansomHouse claiming to have data
 - Persante Health Care – IncRansom leaked videos of sleeping patients
 - Klickitat Valley Health – Kraken, a newer group, listed KVH on its leak site

CISA-FBI Advisory on Medusa Ransomware

Please also refer to the March 3rd Cyber Briefing where we warned about this threat actor and discussed TTPs.

The image is a screenshot of a joint cybersecurity advisory document. At the top, it reads 'JOINT CYBERSECURITY ADVISORY' in large, bold letters. To the right, it says 'TLP:CLEAR' and 'Product ID: AAS-071A'. Below this, it is dated 'March 12, 2025'. The document is co-authored by the FBI, CISA, and MS-ISAC (Multi-State Information Sharing & Analysis Center). The main title is '#StopRansomware: Medusa Ransomware'. A 'Summary' section follows, containing a 'Note' about the advisory's purpose and a box titled 'Actions for Organizations to Take Today to Mitigate Cyber Threats Related to Medusa Ransomware Activity'. This box lists three key actions: 'Mitigate known vulnerabilities', 'Segment networks', and 'Filter network traffic'. The document also includes contact information for reporting suspicious activity and a disclaimer at the bottom.

FBI-CISA published a joint advisory on March 12, 2025, advising threats from Medusa developers and affiliates

- Employs a double extortion model
- Typically recruits initial access brokers (IABs) in cybercriminal forums and marketplaces to obtain initial access
- Uses phishing campaigns and exploit vulnerabilities
- Uses living off the land (LOTL) and legitimate tools including PowerShell and the Windows Command Prompt
- Uses PowerShell detection evasion techniques with increasing complexity and deletes command line history to cover tracks
- Activates remote access software – AnyDesk, Atera, ConnectWise – in combination with Remote Desktop Protocol (RDP) to move laterally
- Exfiltrates data and deploys encryptor

HHS OCR Regulatory Update



Timothy Noonan, deputy director of health information privacy at the Office for Civil Rights (OCR), shared an update on OCR priorities at a session during the Virtual 42nd National HIPAA Summit.

HIPAA Security Rule NPRM:

- Reviewing all 4,745 comments on the HIPAA Security Rule is a key priority

Audit Program

- OCR contacted 50 covered entities and business associates to participate in the 2024-2025 audits
- Focusing on provisions of HIPAA Security Rule most relevant to hacking and ransomware attacks
- Opportunity to address vulnerabilities now rather than under an investigation
- OCR to publish report of the results

Enforcement Actions

- Enforcement under the “Risk Analysis Initiative” continues: 3/21/25 Health Fitness Corporate paid \$227,816 for potential violations

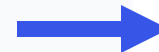
Recommendations

Addressing specific TTPs in current threat environment

- Ensure vulnerabilities are scanned continuously and mitigate high and critical CVEs
- Update Security Awareness training to be in line with current techniques
- Disable or restrict access to Remote Access Tools and other native applications used by TAs
- Review your monitoring, detection and response capabilities – are they sufficient
- Update, test, practice/exercise incident response procedures

Meeting Risk Analysis Requirements

- Review your Risk Analysis and assess whether it...
 - ...has been conducted at the information system level?
 - ...includes all information systems?
 - ...is up to date?
 - ...meets all 9 requirements in OCR's Final Guidance?



[Link to OCR's Final Guidance on Risk Analysis](#)



Fireside Chat

Lessons From the Field: Cybersecurity Trends Across the
Healthcare Ecosystem



Fireside Chat Speakers

Time for
a poll!

- Lessons From the Field: Cybersecurity Trends Across the Healthcare Ecosystem



**Steve Cagle, MBA, HCISPP,
CHISL, CDH-E**

Moderator

Chief Executive Officer

Clearwater



**Jackie Mattingly, Ph.D.,
CHPS, CDH-E, CHISL, CISSP**

Panelist

Sr. Director, Consulting Services,
Regional & Critical Access Hospitals

Clearwater



**Jaime Cifuentes, CISSP, C |
CISO**

Panelist

Director, Consulting Services,
PPM/Ambulatory

Clearwater



**Hal Porter, CISSP, CCSP,
C | CISO, Security+ CE**

Panelist

Director, Consulting Services,
Digital Health/Health IT

Clearwater



Recommendations + Takeaways



Q&A



Upcoming Events



HCCA Annual Compliance Institute
| April 28- May 1, 2025

- Clearwater is excited to participate in HCCA's 29th Annual Compliance Institute, where our experts will lead sessions that dive into critical topics impacting healthcare privacy and compliance. Stop by our booth #327.
- [Click here](#) for our speaking sessions and to register



RSA Conference | April 28-May 1,
2025 | San Francisco, CA

- Members of our team are attending RSA:
- **Dave Bailey** – VP, Consulting Services, Security
- **Laura Martin** – Sr. Account Executive, Hospitals & Health Systems
- **Steve Akers** – CTO & Corporate CISO
- [Click here](#) to meet with our team



McDermott HealthEx | May 6-9,
2025 | Nashville, TN

- Clearwater is proud to be a Patron-Level Sponsor at McDermott HealthEx 2025. This premier event will bring together the healthcare and life sciences industry's most influential leaders, visionaries, and innovators for an unparalleled opportunity to explore the future of healthcare.
- [Click here](#) to register & meet with our team

Upcoming Webinars



Monthly Cyber Briefing | May 1 @ 12:00 CST

- Cyber + regulatory update from Clearwater CEO, Steve Cagle
- Special guest Greg Garcia Executive Director at Health Sector Coordinating Council Cybersecurity Working Group. Greg will discuss his outlook for healthcare policy in 2025, and his recent appearance on Capital Hill testifying to the House Energy and Commerce Subcommittee on Oversight & Investigations about healthcare cybersecurity.
- Those who have registered for this month's Cyber Briefing will be automatically enrolled to participate.



We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.



Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | [linkedin.com/company/clearwater-security-llc/](https://www.linkedin.com/company/clearwater-security-llc/)



Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.