

IN THE EVENT OF A CYBER LOSS:

- 1. Follow your organizations procedures for reporting and responding to an incident.
- 2. Alert authorities, as appropriate.
- 3. Follow the Coalition Claims Reporting Roadmap, on page 2

Call the Coalition Breach Hotline

833-866-1337

Policy Information

Effective Date: July 1, 2023
Policy number: CLP1093970-00

Named Insured: Association of California Water Agencies Joint Powers

Insurance Authority and its Members Scheduled List

4. Notify the following via email:

Coalition: claims@coalitioninc.com

AON Brokers: <u>judy.wang@aon.com</u>; <u>matt.huhn@aon.com</u>;

alex.tokar@aon.com

ACWA JPIA: claims@acwajpia.com

Upon written notice of a claim or incident, Members may engage the Coalition Panel Providers on page 3. Providers include pre-approved expert attorneys and forensics firms.

Coalition - Claims Reporting Roadmap

You are here: Your firm has suffered a security incident. The clock is now ticking. It's time to do right by your customers, employees, shareholders and others. A quick, effective response will help you to avoid lawsuits and regulatory inquiries.

Immediately gather your internal team and review your incident response plan.

Call the Coalition Breach Hotline at **833-866-1337**; then contact the pre-approved expert privacy attorneys to determine legal applicability of actions, to respond to reporting requirements, and to maintain privilege. These lines are monitored seven (7) days a week. Leave a voicemail message. Contact your Aon broker to provide formal notice to Coalition.

A Coalition Claims Specialist will assist with identifying the resources needed to respond to the event and will provide consent as required.

1

Debrief with Coalition Cyber Claims. Some important things to cover:

- · When and how discovered
- Type of event
- · Who attacked
- Extent of attack
- Impact on business
- Type of data at risk
- · # and location of people potentially impacted
- · Ransom demand and threat actor

1

Consult with your expert privacy attorney on the current situation and begin to determine what next steps are necessary.

Engage a pre-approved computer forensics firm to determine existence, cause and scope of the breach.

Engage ransomware response vendor if necessary.

Determine if a public relations or crisis communication firm is required.

Consult with experts to determine if notifications are necessary. If so, decide who needs to be notified and utilize a pre-approved vendor.

After assessing the notification requirements, determine if a call center is required and contact a pre-approved vendor.

Decide if credit or identity monitoring is necessary.

If so, contact the proper credit and identity monitoring firm.

Consider engaging forensic accountant; set up method to track and document cyber-related expenses.

Execute your Response Plan.

ACWA JPIA 9/12/23; Page 2 of 3



Coalition – Pre-Approved Vendors & Resources

Data Breach Response	Litigation	Notification	Forensics / Incident Response	PR & Crisis Management
Cipriani & Werner	BakerHostetler	Epiq	Stroz Friedberg, Aon Cyber Solutions	Infinite Global
Constangy, Brooks, Smith & Prophete	Mullen Coughlin	Experian	Coalition Incident Response	Edelman
Mullen Coughlin	Winget Spadafora & Schwartzberg		Arete	APCO Worldwide
McDonald Hopkins	Cipriani & Werner		Charles River Associates	
	Constangy, Brooks, Smith & Prophete		Kivu Consulting	
			Unit 42	

Forensic Accounting	DDoS Mitigation Providers	
Baker Tilly	Cloudflare	
	Incapsula	
	Google Project Shield	
	Akamai	
	Fastly	

