Cybersecurity Awareness Month

Incident Response Cheat Sheet

Incident Response Team

Function	Internal or External?	Name, Title, Contact Information	Alternate Contact Information
Management	**Internal**		
Information Security	**Internal**		
Information Technology	**Internal**		
Legal	**Internal**		
Accounting/Finance	**Internal**		
Human Resources	**Internal**		
Public Affairs and Media Relations	**Internal**		
Business Continuity	**Internal**		
Physical Security and Facilities Management	**Internal**		
Managed Security Services Provider	**External**		
Outside Counsel	**External - Troutman Pepper**	**Kamran Salour** 949.622.2441 kamran.salour@troutman.com **Sadia Mirza** 949.622.2786 sadia.mirza@troutman.com	**24/7 Incident Response** incident.response@troutman.com

Insurance

Name	Function	Policy Number	Contact Name, Phone, Email Address	Method to Report Incident
	Broker			
	Carrier			

IT/Security Providers

Name	Function	Contact Name, Phone, Email Address
	Managed Security Services Provider	
	Cloud Services Provider	
	Managed Detection and Response Provider	

Privacy/Cybersecurity/Outside Counsel/Breach Coach

Name	Function	Contact Information	Alternate Contact Information
Troutman Pepper	Outside Counsel	**Kamran Salour** 949.622.2441 kamran.salour@troutman.com **Sadia Mirza** 949.622.2786 sadia.mirza@troutman.com	**24/7 Incident Response** incident.response@troutman.com

Forensics, Disaster Recovery, and Threat Actor Negotiations Vendors

Name	Function	Contact Name, Phone, Email Address
	Forensic Vendor	
	PCI Forensic Investigator	
	Ransomware Recovery	
	Threat Actor Negotiations/Bitcoin Payment Provider	
	Ransomware Payment Vendor	

Communication/Notification Vendors

Name	Function	Contact Name, Phone, Email Address
	Mailing and Credit Monitoring	
	Public Relations Firm	

Payment Vendors

Name	Function	Contact Name, Phone, Email Address	Contract Location
	Acquiring Bank		
	Third-Party Payment Processor		
	Payment Card Brand		

Law Enforcement

Agency/Authority	Contact Name	Phone and Email Address

Industry Regulators/Supervisory Authorities

Agency/Authority	Contact Name	Phone and Email Address

Additional Information

Email Provider and License Type	
Number of Email Accounts	
Number of Servers (Physical vs. Virtual) and Location	
Log Retention Limits	
Anti-Virus	
Endpoint Detection and Response (EDR) Tool	
MFA Enabled?	