



Providing Outstanding Service Since 1963

Board of Directors

Janna Orkney, Chair

Susan Pan, Vice Chair

Leon E. Shapiro, Director

Raymond Tjulander, Director

James Wall, Director

September 23, 2019

Board of Directors
Triunfo Water & Sanitation District
Ventura County, California

**CYBER LIABILITY INSURANCE COVERAGE
FOR TRIUNFO WATER & SANITATION DISTRICT**

Summary

At the Triunfo Water & Sanitation District (TWSD) Board meeting on August 26, 2019, the subject of cyber liability insurance was raised by a member of the public in attendance, and the Board directed staff to place that topic on the September meeting agenda for discussion.

Broadly defined, cyber liability is insurance coverage specifically designed to protect a business or organization from a range of threats and incidents relating to a breach event, including:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private;
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online, or social media environment;
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.;
- Defense costs in state or federal regulatory proceedings that involve violations of privacy law; and
- The provision of expert resources and monetary reimbursement to the insured for the out-of-pocket (1st Party) expenses associated with the appropriate handling of the types of incidents listed above.

The term "Cyber" implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats – paper, digital, or otherwise. Please see the "Frequently Asked Questions" document (Attachment A) for additional details on cyber liability insurance.

Financial Impact

Currently, TWSD does not have cyber liability insurance coverage in its risk management portfolio. Staff contacted representatives at Tolman Wiker Insurance Services, the brokerage that administers TWSD's property insurance coverage, and received quotations for coverage levels that are summarized on the quotation forms (Attachment B). Annual premium costs would be:

\$1,000,000 maximum liability: \$5,524

\$2,000,000 maximum liability: \$7,044

These amounts are not included in the TWSD Fiscal Year 2019-20 budget; therefore, purchase of cyber liability insurance coverage would necessitate Board authorization of an appropriate budget adjustment.

Recommendation

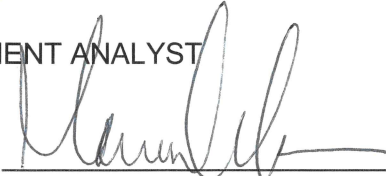
It is recommended that the Board evaluate the information on cyber liability insurance coverage presented above and in the attached documents and direct staff accordingly.

If you have questions, please call me at (805) 658-4608 or email sandywarren@vrsd.com.



SANDY WARREN – MANAGEMENT ANALYST

REVIEWED AND APPROVED:



Mark Norris - General Manager

Attachments:

Attachment A - Frequently Asked Questions

Attachment B - Quotation Forms

Frequently Asked Questions

Do you have any questions about your insurance? The frequently asked questions below are here to help you make an informed decision.

What is Cyber Liability Insurance?

"Cyber" Liability is insurance coverage specifically designed to protect a business or organization from a range of threats and incidents relating to a breach event including:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online or social media environment
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.
- Defense costs in State or Federal regulatory proceedings that involve violations of privacy law; and
- The provision of expert resources and monetary reimbursement to the Insured for the out-of-pocket (1st Party) expenses associated with the appropriate handling of the types of incidents listed above

The term "Cyber" implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats – paper, digital or otherwise.

What does Privacy Liability (including Employee Privacy) cover?

The Privacy Liability aspect of the insuring agreement in our policy goes beyond providing liability protection for the Insured against the unauthorized release of Personally Identifiable Information (PII), Protected Health Information (PHI), and corporate confidential information of third parties and employees, like most popular "Data Breach" policies. Rather, our policy provides true Privacy protection in that the definition of **Privacy Breach** includes violations of a person's right to privacy, etc. Because information lost in every data breach may not fit State or Federal-specific definitions of PII or PHI, our policy broadens coverage to help fill these potentially costly gaps. This is a key provision that truly sets the RPS policy apart from others.

What does Privacy Regulatory Claims Coverage cover?

The Privacy Regulatory Claims Coverage insuring agreement provides coverage for both legal defense and the resulting fines/penalties emanating from a **Regulatory Claim** made against the Insured, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation with respect to privacy regulations.

Does this policy cover regulatory investigations and/or fines related to GDPR privacy violations?

The BCS cyber policy has always provided broad **Regulatory Claim** coverage that would contemplate defense and penalties associated with unintentional violations of domestic and foreign privacy statutes. In accordance with the implementation of the EU's General Data Protection Regulation, BCS added clarifying language to the policy form under the definitions of **Privacy Regulations** and **Private Information** to specifically reference coverage for GDPR by name (subject to policy terms and conditions). It is important to note that fines and penalties may not be insurable by law in certain U.S. States and in certain foreign countries, including some member countries of the European Union.

What does Security Breach Response Coverage cover?

This 1st Party coverage reimburses an Insured for costs incurred in the event of a security breach of personal, non-public information of their customers or employees. Examples include:

- The hiring of a public relations consultant to help avert or mitigate damage to the Insured's brand
- IT forensics, customer notification and 1st Party legal expenses to determine the Insured's obligations under applicable Privacy Regulations
- Credit monitoring expenses for affected customers for up to 12 months and longer if circumstances require.

Our policy can also extend coverage even in instances where there is no legal duty to notify if the Insured feels that doing so will mitigate potential brand damage (such voluntary notification requires prior written consent).

What does Security Liability cover?

The Security Liability insuring agreement provides coverage for the Insured for allegations of a **Security Wrongful Act**, including:

- The inability of a third-party, who is authorized to do so, to gain access to the Insured's computer systems
- The failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as phishing that results in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party
- Protects against liability associated with the Insured's failure to prevent transmission of malicious code from their **Computer System** to a third party's **Computer System**

What does Multimedia Liability cover?

The Multimedia Liability insuring agreement provides coverage against allegations that include:

- Defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the Insured's communication of **Media Content** in electronic (website, social media, etc.) or non-electronic forms

Other "Cyber" insurance policies often limit this coverage to content posted to the Insured's website. Our policy extends what types of media are covered as well as the formats where this information resides.

What does Cyber Extortion cover?

The **Cyber Extortion** insuring agreement provides:

- Expense and payments (including ransom payments if necessary) to a third party to avert potential damage threatened against the Insured such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information

Ransomware is among the most reported types of cybersecurity incidents. Verizon's 2018 Data Breach Investigations Report (DBIR) indicated that ransomware is the most common type of malware, found in 39 percent of malware-related data breaches – double of the amount reported in last year's DBIR. Investigation and other expenses associated with ransomware events are contemplated under the **Cyber Extortion** insuring agreement. Additionally, Symantec's 2018 Internet Security Threat Report indicated that 2017 brought a 46% increase in new ransomware variants. Having the proper team in place to help you navigate the intricacies of a ransomware attack is critical and the RPSCyber policy provides this through the **Cyber Extortion** coverage

What does Business Income and Digital Asset Restoration cover?

The Business Income and Digital Asset Restoration insuring agreement provides for lost earnings and expenses incurred because of a **Network Disruption**, or, an authorized third-party's inability to access a **Computer System**. The policy will also cover for lost business as a result of a loss of reputation caused by any failure or disruption to **Computer Systems**. **Restoration Costs** to restore or recreate digital (not hardware) assets to their pre-loss state are provided for as well. What's more, the definition of **Computer System** is broadened to include not only systems under the Insured's direct control, but also systems under the control of a **Service Provider** with whom the Insured contracts to hold or process their digital assets. Most competing Cyber insurance forms require that a **Security Breach** take place in order for Business Interruption coverage to respond. The BCS form is unique in that the definition of **Network Disruption** is extremely broad and includes any unplanned failure, interruption or degradation of the operation of your **Computer System** or the **Computer System** of an IT service provider – whether it was caused by a **Security Breach** or otherwise. The BCS policy further differentiates itself by taking this expansion of coverage a step further. In addition to IT service providers, coverage for **Network Disruption** is provided (on a sub-limited basis) to **Outsourced Providers**, that is, any provider, other than an IT **Service Provider**, that provides services (other than IT services) for you, pursuant to a written contract. This expanded coverage is offered without the need for additional underwriting.

What is "PCI-DSS Assessment" coverage?

The Payment Card Industry Data Security Standard (PCI-DSS) was established in 2006 through a collaboration of the major credit card brands as a means of bringing standardized security best practices for the secure processing of credit card transactions. Merchants and service providers must adhere to certain goals and requirements in order to be "PCI Compliant," and certain specific agreements, may subject an Insured to an "assessment" for breach of such agreements. The RPS Cyber Policy responds to **PCI Assessments** as well as claims expenses in the wake of a breach involving cardholder information. Additionally, this coverage provides for expenses associated with a mandatory audit performed by a Qualified Security Assessor (QSA), certified by the PCI Security Standards Council, to show you are PCI DSS compliant, following a **Security Breach**.

What is Cyber Deception cover?

The **Cyber Deception** extension is purchased for an additional premium if the applicant is eligible. The extension provides coverage for the intentional misleading of the Applicant by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the Applicant believing it to be genuine. This is commonly known as spear-phishing or social engineering, and, along with ransomware events, is among the most reported incidents to the BCS Cyber policy. Many Cyber policies offering this coverage require that the insured call back, or, attempt to verify the request's authenticity via a method other than the original means. In other words, if a request to transfer money to a different bank routing number is received via email, other Cyber policies may require that the person receiving the email attempt to verify the request also via telephone before authorizing the transfer of money. While the application process asks a question regarding controls in place for this, the BCS policy differentiates itself further by not requiring this of insureds in the policy wording.

What is Telephone Hacking coverage?

Telephone Hacking coverage is included in the **Electronic Fraud** sub-section of the BCS policy. It provides a sub-limit of coverage for the intentional, unauthorized and fraudulent use of your **Telecommunications Services** (ie: telephone, fax, broadband or other data transmission services that you purchase from third parties) that results in unauthorized calls or unauthorized use of your bandwidth.

What is Funds Transfer Fraud coverage?

Funds Transfer Fraud coverage is available in the **Electronic Fraud** sub-section of the BCS policy for insureds who are NOT classified as Financial Institutions (Financial Institutions includes Community, State or Credit Unions, as well as National financial institutions, banks, etc.) For those organizations who are not in the financial institution classification, the coverage provides coverage for unauthorized electronic funds transfer, theft of your money or other financial assets from your bank by electronic means, theft of your money or other financial assets from your corporate credit cards by electronic means, or any fraudulent manipulation of electronic documentation while stored on your **Computer System**. This should not be confused with **Cyber Deception** coverage which requires a willful release of funds (not theft) based on a fraudulent instruction the insured believes to be true.

Who is RPS?

With more than 2,000 employees throughout the United States, Risk Placement Services empowers insurance agents and brokers like yours with product and industry expertise, and access to exclusive Property & Casualty insurance coverage for their clients throughout the country. RPS is the exclusive Managing General Agent for the specialized Cyber insurance quotation your agent has provided herein. RPS is consistently recognized by Business Insurance magazine as the nation's largest Managing General Agency. RPS is also honored to be named the winner of the Business Insurance "2018 Insurtech Initiative of the Year" award. Your agent's decision to partner with RPS speaks of their desire to provide your organization with the best insurance solutions available in the marketplace today.

How is this policy better than other options in the marketplace?

As with any insurance policy, what sets our coverage apart lies in the definitions and exclusions in the policy. The RPS Cyber Policy offers broader definitions of critical terms such as **Privacy Breach**, **Computer System**, and **Media Content**. These definitions, along with the absence of some industry-standard exclusions and a drastically streamlined application process, make this policy more comprehensive and easier to access than the typical Cyber policy available from traditional sources.

Isn't this already covered under most business insurance plans?

The short answer is "No". While liability coverage for data breach and privacy claims has been found in limited instances through General Liability, Commercial Crime and some D&O policies, these forms were not intended to respond to the modern threats posed in today's 24/7 information environment. Where coverage has been afforded in the past, carriers (and the ISO) are taking great measures to include exclusionary language in form updates that make clear their intentions of not covering these threats. Additionally, even if coverage can be found in rare instances through other policies, they lack the expert resources and critical 1st Party coverages that help mitigate the financial, operational and reputational damages a data breach can inflict on an organization.

Are businesses required to carry this coverage?

While there is presently no law that requires a business or organization to carry Cyber Liability, there is a national trend in business contracts for proof of this coverage. In addition, the SEC and other regulatory bodies are encouraging disclosure of this coverage as a way of demonstrating sound information security risk management. Laws such as HIPAA-HITECH, GDPR, Gramm-Leach-Bliley and state-specific data breach laws are continually driving demand as requirements for notification in the wake of a data breach become more expensive, and expectations around the level of response by an impacted organization are increased.

Do small businesses need this coverage?

A recent Ponemon Institute report uncovered that 50% of small and medium sized US businesses had suffered a data breach, with 55% suffering a cyber-attack, with the most prevalent attack being non-sophisticated phishing attempts. The US National Cyber Security Alliance has advised that 60% of small companies are out of business within 6 months after being hacked. While breaches involving public corporations and government entities garner the vast majority of headlines, it is the small business that can be most at risk. With lower information security budgets, limited personnel and greater system vulnerabilities, small businesses are increasingly at risk for a data breach. In the past, many small business owners in the SME space were reluctant to purchase Cyber liability insurance coverage because they did not see themselves as data rich targets. Today's trends are showing that much of the data breach and ransomware attacks in today's business environment are indiscriminant of industry or size. Random attacks distributed to thousands of unknown recipients with the hopes of snaring just a limited number have caused business owners of all sizes and descriptions to re-think their approach to this huge risk and purchase insurance to mitigate the effects.

If e-commerce functions such as payment processing or data storage are outsourced, is this coverage still needed?

The responsibility to notify customers of a data breach or legal liabilities associated with protecting customer data, remain the responsibility of the Insured. Generally speaking, business relationships exist between Insureds and their customers, not their customers and the back-office vendors the Insured uses to assist them in their operations. Outsourcing business critical functions such as payment processing, data storage, website hosting, etc. can help insulate Insureds from risk, however, the contractual agreement wording between Insureds, their customers and the vendors with whom they do business will govern the extent to which liability is assigned in specific incidents.

What is the cost of not buying the coverage and self-insuring a data breach?

The Ponemon Institute, a well-known research firm, publishes an annual "Cost of a Data Breach" report. In partnership with IBM, the 2017 report indicated that the average cost paid for each lost or stolen record is \$141. These numbers are reflective of both the indirect expenses associated with a breach (time, effort and other organizational resources spent during the data breach resolution, customer churn, etc.), as well as direct expenses (customer notification, credit monitoring, forensics, hiring a law firm, etc.).

While there has been a decrease in the average cost paid for each lost or stolen record since 2016, (down from \$158), the average size of a breach has increased to 1.8 times the size of breaches last year. So, despite decreasing average costs per record, more records are being lost which means an increasing cost to businesses. More information can be found in the "2017 Cost of Data Breach Study: Global Overview" at www.ponemon.org.

In addition, the cost of breaches has evolved from just the cost of notification to now include ransom demands, business income loss, theft, and associated liability costs. These additional factors have also contributed to driving up the potential financial impact of a breach incident.

Who is the insurance carrier?

The BCS Cyber and Privacy Liability Policy is underwritten by BCS Insurance Company and powered by and with the backing of certain syndicates at Lloyd's of London. BCS Insurance Company is a licensed, admitted insurance company in all states and the District of Columbia. The BCS Cyber policy is admitted in every state except VT. BCS Insurance Company provides value through a solid foundation of strong governance, national and international capabilities and product and industry expertise and is rated A- (Excellent) by A.M. Best. BCS Insurance has been in business for over 60 years. It is a wholly owned subsidiary of BCS Financial Corporation which, in turn, is owned by all Blue Cross Blue Shield primary licensees. BCS Insurance Company's relationship with certain syndicates at Lloyd's of London brings additional strength, stability and industry-leading expertise to the RPS cyber insurance program. BCS was recognized by S&P Global as the #6 underwriter of cybersecurity insurance in 2017, according to direct written premium, and the #3 market for in-force policies.

What is the claims-handling process?

A 24-hour data breach hotline is available to report incidents or even suspected incidents. As soon as you suspect a data breach incident or receive notice of a claim, you should call the hotline listed in your policy. This hotline is manned by Baker Hostetler, a world-wide leading privacy law firm with experience in handling thousands of data breach events. Immediately after calling the hotline, you are required to send notice to Clyde & Co., the designated legal firm that has been contracted to triage initial notices in this regard. This can be done by sending an email with a brief description of the incident, including your contact information, to the claims-reporting email address listed in your policy. Your RPS broker will receive notification of the incident (or any third-party claim) as well. It is critical that you immediately report any and all incidents that you believe could give rise to a claim of any kind under this policy.

What if there are questions that are not answered here?

Please contact your preferred Cyber Professional who will assist you with any questions you may have.



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

Attachment B

(A stock insurance company, herein the "Company")

Policy No. RPS-Q-0706012M/1

Cyber and Privacy Liability Insurance Policy

94.111 (06/18)

NOTICE: THE POLICY CONTAINS ONE OR MORE COVERAGES. CERTAIN COVERAGES ARE LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED AND NOTIFIED TO US DURING THE POLICY PERIOD AS REQUIRED. CLAIM EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION (S). PLEASE READ THIS POLICY CAREFULLY.

POLICY DECLARATIONS

ITEM 1.	NAMED INSURED	Triunfo Water & Sanitation District
	ADDRESS	1001 Partridge Dr Ste 150 , Ventura, California, 93003-0704
ITEM 2.	POLICY PERIOD	FROM: September 12, 2019 TO: September 12, 2020 (12:01 A.M. Standard time at the address shown in Item 1.)
ITEM 3.	POLICY LIMITS OF LIABILITY AND COVERAGES PURCHASED	I. Aggregate Limit of Liability: \$1,000,000 (Aggregate for Each and Every Claim or Event including Claims Expenses) II. Sublimit of Liability for Individual Coverage(s) Purchased: \$1,000,000 "Nil" or "N/A" Sublimit of Liability for any coverage indicates that the coverage was not purchased

COVERAGE	PER CLAIM SUBLIMIT OF LIABILITY INCLUDES CLAIM EXPENSES	AGGREGATE SUBLIMIT OF LIABILITY
A. Privacy Liability (including Employee Privacy)	\$1,000,000	\$1,000,000
B. Privacy Regulatory Claims Coverage	\$1,000,000	\$1,000,000
C. Security Breach Response Coverage	\$1,000,000	\$1,000,000
D. Security Liability	\$1,000,000	\$1,000,000
E. Multimedia Liability	\$1,000,000	\$1,000,000
F. Cyber Extortion	\$1,000,000	\$1,000,000
G. Business Income and Digital Asset Restoration	\$1,000,000	\$1,000,000
H. PCI DSS Assessment	\$1,000,000	\$1,000,000



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

I. Electronic Fraud

1. Telephone Hacking	\$100,000	\$100,000
2. Funds Transfer Fraud	\$100,000	\$100,000

ITEM 4. RETENTION (including Claims Expenses):

COVERAGE	EACH CLAIM
A. Privacy Liability (including Employee Privacy)	\$5,000
B. Privacy Regulatory Claims Coverage	\$5,000
C. Security Breach Response Coverage	\$5,000
D. Security Liability	\$5,000
E. Multimedia Liability	\$5,000
F. Cyber Extortion	\$5,000
G. Business Income and Digital Asset Restoration	\$5,000 / 10 hrs waiting period
H. PCI DSS Assessment	\$5,000
I. Electronic Fraud	
1. Telephone Hacking	\$5,000
2. Funds Transfer Fraud	\$5,000

ITEM 5. PREMIUM	\$5,019.00
CYBER DECEPTION PREMIUM:	\$450.00 (IF ELECTED)
TRIA PREMIUM:	\$55.00 (IF ELECTED IS 1% OF THE TOTAL PREMIUM)
TOTAL:	\$5,524.00

ITEM 6. TERRITORIAL LIMITS	Worldwide
-----------------------------------	-----------

ITEM 7. RETROACTIVE DATE	Full Prior Acts
---------------------------------	-----------------

ITEM 8. NOTICE OF CLAIM	<u>2 Steps:</u> 1. Call Baker Hostetler at the 24 Hour Security Breach Hotline: 1-866-288-1705 2. File your claim with:
--------------------------------	--

rpscyberclaims@clydeco.us
Clyde & Co. US LLP
101 Second Street, 24th Floor
San Francisco CA 94105
USA

ITEM 9. SERVICE OF SUIT	Risk Situated in California:
--------------------------------	------------------------------



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

Eileen Ridley
FLWA Service Corp.
c/o Foley & Lardner LLP
555 California Street, Suite 1700, San Francisco, CA 94104-1520

Risks Situated in All Other States:
Mendes & Mount
750 Seventh Avenue, New York, NY 10019

ITEM 10. CHOICE OF LAW

California

ITEM 11. WAITING PERIOD:

10 hrs waiting period

**FORMS AND ENDORSEMENTS
EFFECTIVE AT INCEPTION**

94.200 (06/17) CYBER AND PRIVACY LIABILITY POLICY FORM
Cyber Deception Endorsement (If elected)
94.102 (01 15) Nuclear Incident Exclusion
94.103 (01 15) Radioactive Contamination Exclusion
94.805 (06/17) Breach Response Team Endorsement
94.801 (06/17) CALIFORNIA Amendatory
94.527 (06/18) Coverage Enhancements Endorsement
94.528 (06/18) FTF Coverage Endorsement
BCSI-X009 CA (01 15) CA Premium Return Notice
94.551 (01 15) Coverage for Certified Acts of Terrorism (Included only if
Terrorism coverage is elected at 1% additional premium)
94.552 CA (01 15) War and Terrorism Endorsement



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

(A stock insurance company, herein the "Company")

Policy No. RPS-Q-0706014M/1

Cyber and Privacy Liability Insurance Policy

94.111 (06/18)

NOTICE: THE POLICY CONTAINS ONE OR MORE COVERAGES. CERTAIN COVERAGES ARE LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED AND NOTIFIED TO US DURING THE POLICY PERIOD AS REQUIRED. CLAIM EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION (S). PLEASE READ THIS POLICY CAREFULLY.

POLICY DECLARATIONS

ITEM 1.	NAMED INSURED	Triunfo Water & Sanitation District
	ADDRESS	1001 Partridge Dr Ste 150 , Ventura, California, 93003-0704
ITEM 2.	POLICY PERIOD	FROM: September 12, 2019 TO: September 12, 2020 (12:01 A.M. Standard time at the address shown in Item 1.)
ITEM 3.	POLICY LIMITS OF LIABILITY AND COVERAGES PURCHASED	I. Aggregate Limit of Liability: \$2,000,000 (Aggregate for Each and Every Claim or Event including Claims Expenses) II. Sublimit of Liability for Individual Coverage(s) Purchased: \$2,000,000 "Nil" or "N/A" Sublimit of Liability for any coverage indicates that the coverage was not purchased

COVERAGE	PER CLAIM SUBLIMIT OF LIABILITY INCLUDES CLAIM EXPENSES	AGGREGATE SUBLIMIT OF LIABILITY
A. Privacy Liability (including Employee Privacy)	\$2,000,000	\$2,000,000
B. Privacy Regulatory Claims Coverage	\$2,000,000	\$2,000,000
C. Security Breach Response Coverage	\$2,000,000	\$2,000,000
D. Security Liability	\$2,000,000	\$2,000,000
E. Multimedia Liability	\$2,000,000	\$2,000,000
F. Cyber Extortion	\$2,000,000	\$2,000,000
G. Business Income and Digital Asset Restoration	\$2,000,000	\$2,000,000
H. PCI DSS Assessment	\$2,000,000	\$2,000,000



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

I. Electronic Fraud

1. Telephone Hacking	\$100,000	\$100,000
2. Funds Transfer Fraud	\$100,000	\$100,000

ITEM 4. RETENTION (including Claims Expenses):

COVERAGE	EACH CLAIM
A. Privacy Liability (including Employee Privacy)	\$5,000
B. Privacy Regulatory Claims Coverage	\$5,000
C. Security Breach Response Coverage	\$5,000
D. Security Liability	\$5,000
E. Multimedia Liability	\$5,000
F. Cyber Extortion	\$5,000
G. Business Income and Digital Asset Restoration	\$5,000 / 10 hrs waiting period
H. PCI DSS Assessment	\$5,000
I. Electronic Fraud	
1. Telephone Hacking	\$5,000
2. Funds Transfer Fraud	\$5,000

ITEM 5. PREMIUM	\$6,524.00
CYBER DECEPTION PREMIUM:	\$450.00 (IF ELECTED)
TRIA PREMIUM:	\$70.00 (IF ELECTED IS 1% OF THE TOTAL PREMIUM)
TOTAL:	\$7,044.00

ITEM 6. TERRITORIAL LIMITS Worldwide

ITEM 7. RETROACTIVE DATE Full Prior Acts

ITEM 8. NOTICE OF CLAIM 2 Steps:

1. Call Baker Hostetler at the 24 Hour Security Breach Hotline:
1-866-288-1705
2. File your claim with:

rpscopyberclaims@clydeco.us
Clyde & Co. US LLP
101 Second Street, 24th Floor
San Francisco CA 94105
USA

ITEM 9. SERVICE OF SUIT Risk Situated in California:



BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

Eileen Ridley
FLWA Service Corp.
c/o Foley & Lardner LLP
555 California Street, Suite 1700, San Francisco, CA 94104-1520

Risks Situated in All Other States:
Mendes & Mount
750 Seventh Avenue, New York, NY 10019

ITEM 10. CHOICE OF LAW

California

ITEM 11. WAITING PERIOD:

10 hrs waiting period

**FORMS AND ENDORSEMENTS
EFFECTIVE AT INCEPTION**

94.200 (06/17) CYBER AND PRIVACY LIABILITY POLICY FORM
Cyber Deception Endorsement (If elected)
94.102 (01 15) Nuclear Incident Exclusion
94.103 (01 15) Radioactive Contamination Exclusion
94.805 (06/17) Breach Response Team Endorsement
94.801 (06/17) CALIFORNIA Amendatory
94.527 (06/18) Coverage Enhancements Endorsement
94.528 (06/18) FTF Coverage Endorsement
BCSI-X009 CA (01 15) CA Premium Return Notice
94.551 (01 15) Coverage for Certified Acts of Terrorism (Included only if
Terrorism coverage is elected at 1% additional premium)
94.552 CA (01 15) War and Terrorism Endorsement