

State: District of Columbia **Filing Company:** Arch Insurance Company
TOI/Sub-TOI: 17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability
Product Name: Network Security and Data Breach Endorsement Revision
Project Name/Number: ESIP General Liability Form Revision/ARCH-16-177

Filing at a Glance

Company: Arch Insurance Company
Product Name: Network Security and Data Breach Endorsement Revision
State: District of Columbia
TOI: 17.0 Other Liability-Occ/Claims Made
Sub-TOI: 17.0001 Commercial General Liability
Filing Type: Form
Date Submitted: 11/17/2016
SERFF Tr Num: AICO-130810784
SERFF Status: Assigned
State Tr Num:
State Status:
Co Tr Num: ARCH-16-177
Effective Date: On Approval
Requested (New):
Effective Date: On Approval
Requested (Renewal):
Author(s): Kathleen Marie Campbell, Tara Martin, Alex Ty
Reviewer(s): Angela King (primary)
Disposition Date:
Disposition Status:
Effective Date (New):
Effective Date (Renewal):

State: District of Columbia **Filing Company:** Arch Insurance Company
TOI/Sub-TOI: 17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability
Product Name: Network Security and Data Breach Endorsement Revision
Project Name/Number: ESIP General Liability Form Revision/ARCH-16-177

General Information

Project Name: ESIP General Liability Form Revision	Status of Filing in Domicile: Pending
Project Number: ARCH-16-177	Domicile Status Comments: This filing is pending in Missouri.
Reference Organization:	Reference Number:
Reference Title:	Advisory Org. Circular:
Filing Status Changed: 11/17/2016	
State Status Changed:	Deemer Date:
Created By: Alex Ty	Submitted By: Alex Ty
Corresponding Filing Tracking Number:	

Filing Description:

Arch Insurance Company (Arch) is submitting for your review and approval a revised General Liability form filing for use with its Emergency Services Insurance Program (ESIP) in your state.

Form GL 4000 is an optional endorsement selected at the request of the insured. It provides network security and data breach coverage for events first discovered during the policy period or any extended reporting period.

We are revising exclusion 'k' in order to clarify our intent to give back coverage for an insured to be able to file suit against a named insured specifically for a privacy event.

Enclosed for your review is:

GL 4000 10 16 – Network Security and Data Breach

A marked up version of the revised form has been provided to show the proposed change.

There is no rate impact associated with this form

Company and Contact

Filing Contact Information

Tara Martin, Compliance Analyst	tmartin@archinsurance.com
300 - Plaza 3 - Third Floor	201-743-4113 [Phone]
Jersey City, NJ 07311	917-591-4576 [FAX]

Filing Company Information

Arch Insurance Company	CoCode: 11150	State of Domicile: Missouri
Harborside 3	Group Code: 1279	Company Type: Property & Casualty
210 Hudson Street	Group Name: Arch Insurance Group	State ID Number:
Suite 300	FEIN Number: 43-0990710	
Jersey City, NJ 07311		
(201) 743-4115 ext. [Phone]		

Filing Fees

Fee Required?	No
Retaliatory?	No

State: District of Columbia **Filing Company:** Arch Insurance Company

TOI/Sub-TOI: 17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability

Product Name: Network Security and Data Breach Endorsement Revision

Project Name/Number: ESIP General Liability Form Revision/ARCH-16-177

Fee Explanation:

State: District of Columbia**Filing Company:**

Arch Insurance Company

TOI/Sub-TOI: 17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability**Product Name:** Network Security and Data Breach Endorsement Revision**Project Name/Number:** ESIP General Liability Form Revision/ARCH-16-177

Form Schedule

Item No.	Schedule Item Status	Form Name	Form Number	Edition Date	Form Type	Form Action	Action Specific Data		Readability Score	Attachments
							Previous Filing Number:	Replaced Form Number:		
1		NETWORK SECURITY AND DATA BREACH ENDORSEMENT	GL 4000	10 16	END	Replaced	REGU-129394680	GL 4000 01 14	44.500	GL 4000 10 16 - NETWORK SECURITY AND DATA BREACH ENDORSEMENT .pdf

Form Type Legend:

ABE	Application/Binder/Enrollment	ADV	Advertising
BND	Bond	CER	Certificate
CNR	Canc/NonRen Notice	DEC	Declarations/Schedule
DSC	Disclosure/Notice	END	Endorsement/Amendment/Conditions
ERS	Election/Rejection/Supplemental Applications	OTH	Other

ARCH INSURANCE COMPANY

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

NETWORK SECURITY AND DATA BREACH ENDORSEMENT

Insured:	Policy No.:	Effective Date:
----------	-------------	-----------------

NOTICE: EXCEPT AS OTHERWISE PROVIDED, THE COVERAGE PROVIDED BY THIS ENDORSEMENT IS LIMITED TO ONLY THOSE EVENTS THAT ARE FIRST DISCOVERED AND REPORTED WHILE THIS POLICY IS IN FORCE OR DURING ANY EXTENDED REPORTING PERIOD. VARIOUS PROVISIONS IN THIS ENDORSEMENT RESTRICT COVERAGE. PLEASE READ THE ENTIRE ENDORSEMENT CAREFULLY TO DETERMINE RIGHTS, DUTIES AND WHAT IS AND IS NOT COVERED.

This endorsement modifies the insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE FORM

SCHEDULE

Coverage E – Network Security and Data Breach Liability

Network Security and Data Breach Liability Each Event Limit	\$
Network Security and Data Breach Liability Aggregate Limit	\$
Network Security and Data Breach Liability Retroactive Date	

Coverage F – Privacy Event Mitigation Expense

Privacy Event Mitigation Expense Each Event Limit	\$
Privacy Event Mitigation Expense Aggregate Limit	\$
Privacy Event Mitigation Expense Retroactive Date	

A. The following are added to **Section I – Coverages**:

1. Coverage E – Network Security and Data Breach Liability

Insuring Agreement

a. We will pay those sums that the insured becomes legally obligated to pay as monetary damages because of a "network security or data breach event" to which this insurance applies. We have the right and duty to defend the insured against any "suit" seeking those monetary damages. We have no duty to defend the insured against any "suit" not seeking monetary damages. We also have no duty to defend the insured against any "suit" based upon, arising out of, or attributable to a "network security or data breach event" to which this insurance does not apply. However, at our discretion, we have the right to investigate any "network security or data breach event" and settle any claim or "suit" that may result. But:

(1) The amount we will pay for monetary damages is limited as described below in **Section C. Limits Of Insurance**;

(2) Our right and duty to defend ends when we have used up the applicable limit of insurance in the payment of judgments or settlements.

No other obligation or liability to pay sums or perform acts or services is covered unless explicitly provided for under **Supplementary Payments – Coverages A, B and E**.

b. This insurance applies to a "network security or data breach event" only if:

(1) Such "network security or data breach event" takes place in the "coverage territory"; and

(2) Such "network security or data breach event" did not result from an act, error or omission that occurred before the Network Security and Data Breach Liability Retroactive Date shown in the schedule or after the end of the policy period; and

- (3) The "network security or data breach event" is first discovered in accordance with Paragraph c. below during the policy period or any Extended Reporting Period we provide under **4. Extended Reporting Periods**; and
- (4) Written notice is received by us of the "network security or data breach event" within sixty (60) days of its first discovery or before the end of any Extended Reporting Period we provide under **4. Extended Reporting Periods**, whichever is earlier.

c. First Discovery and Related Events or Acts

(1) First Discovery

A "network security or data breach event" will be deemed to have been discovered at the earliest of the following times:

- (a) When such "network security or data breach event" is discovered and recorded by any insured, or by us, whichever comes first; or
- (b) When the insured becomes aware of an act, error or omission that may subsequently result in a "network security or data breach event", and you give written notice to us, as described in **Section IV – Conditions**, of such circumstances as soon as practicable but no later than:
 - (i) Sixty (60) days after becoming aware; or
 - (ii) The end of any applicable Extended Reporting Period; whichever is earlier.

(2) Related Events

All related "network security or data breach events" will be considered one event and will be considered first discovered when the first of such related events is discovered.

Related "network security or data breach events" include all "network security or data breach events" that are logically or causally connected by a common nexus of facts, circumstances, situations, events, transactions, causes or acts.

2. Coverage F – Privacy Event Mitigation Expense

Insuring Agreement

- a. We will pay "privacy event mitigation expenses" incurred by the insured, provided such expenses arise directly out of a "privacy event" for which coverage is not otherwise excluded. But the amount we will pay is limited as described below in **Section C – Limits Of Insurance**;

No other obligation or liability to pay sums or perform acts or services is covered.

- b. This insurance applies to "privacy event mitigation expenses" only if:

- (1) The "privacy event" takes place in the "coverage territory"; and
- (2) The "privacy event" did not result from an act, error or omission that occurred before the Privacy Event Mitigation Expense Retroactive Date shown in the schedule or after the end of the policy period; and
- (3) The "privacy event" is first discovered in accordance with Paragraph c. below during the policy period or any Extended Reporting Period we provide under **4. Extended Reporting Periods**; and
- (4) Written notice is received by us of the "privacy event" within sixty (60) days of its first discovery or before the end of any Extended Reporting Period we provide under **4. Extended Reporting Periods**, whichever is earlier.

c. First Discovery and Related Events or Acts

(1) First Discovery

A "privacy event" will be deemed to have been discovered at the earliest of the following times:

- (a) When such "privacy event" is discovered and recorded by any insured, or by us, whichever comes first; or
- (b) When you become aware of an act, error or omission that may subsequently result in a "privacy event", and you give written notice to us, as described in **Section IV – Conditions**, of such circumstances as soon as practicable but no later than:
 - (i) Sixty (60) days after becoming aware; or
 - (ii) The end of any applicable Extended Reporting Period; whichever is earlier.

(2) Related Events

All related "privacy events" will be considered one event and will be considered first discovered when the first of such related events is discovered.

Related "privacy events" include all "privacy events" that are the same, related or continuous, or that arise from a common nucleus of facts, circumstances, events or acts.

3. Exclusions

This insurance does not apply to:

- a. Damages, loss or expense arising directly or indirectly from:
 - (1) Any shortcoming in data security that the insured knew about prior to the inception of this policy for which you failed to take corrective action within a reasonable time, not to exceed sixty (60) days;
 - (2) The insured's failure to comply with all the data security standards issued by credit card issuers or financial institutions with whom you transact business, if you process, store or handle credit card information;
 - (3) The insured's failure to take reasonable steps to use, design, maintain and upgrade your data security; or
 - (4) The inability to use or lack of performance of software:
 - (a) Due to expiration, cancellation or withdrawal of such software;
 - (b) That has not yet been released from its development stage; or
 - (c) That has not passed all test runs or proven successful in applicable daily operations.
- b. Damages, loss or expense arising directly or indirectly from:
 - (1) The illegal, unauthorized or wrongful collection of "personally identifiable information" including but not limited to collection of "personally identifiable information" using cookies or malware, if committed by or with the knowledge of the insured; or
 - (2) The failure to provide required notice that such "personally identifiable information" is being collected.
- c. Damages, loss or expense arising directly or indirectly from the seizure, confiscation, expropriation, nationalization or destruction of a "computer system" by order of any governmental authority.
- d. Any "network security or data breach event" or "privacy event" that results from an act, error or omission that takes place prior to the inception date of this policy if the insured knew or reasonably should have foreseen that such act, error or omission would give rise to a claim or "privacy event mitigation expense".
- e. Damages, loss or expense based upon, attributable to, arising out of, in consequence of, or in any way related to litigation or any administrative or regulatory proceedings if such litigation or administrative or regulatory proceedings were initiated prior to or were pending on the inception date of this policy.
- f. "Bodily injury", "property damage" or "personal and advertising injury".
- g. Violation or invasion of any right of privacy except as a result of a "privacy event".
- h. Breach of contract by an insured or liability assumed by an insured under any contract or agreement. This exclusion does not apply to liability the insured would have in the absence of the contract or agreement.
- i. Fines or penalties imposed by any federal, state or local governmental authority.
- j. Any fraudulent, dishonest, malicious, or criminal act by the insured.
- k. Any "claim" or "suit" brought by or on behalf of any insured against any other insured; provided, however, that this exclusion will not apply to any otherwise covered "claim" or "suit" brought by or on behalf of any insured against a Named Insured arising out of a "privacy event", provided that such insured is not involved in any manner with any such "privacy event".
- l. Costs or expenses incurred by the insured to comply with any demand or order by any federal, state or local governmental authority other than those provided under **Coverage F – Privacy Event Mitigation Expense**.
- m. Any cost to comply with any injunctive or other non-monetary or declaratory relief or any agreement to provide such relief.

- n. Any claim or "suit" alleging, based upon, arising out of, or resulting from, directly or indirectly, any unsolicited electronic faxes, emails, telephone calls or unsolicited communications, including but not limited to claims arising out of unsolicited electronic messages, chat room postings, bulletin board postings, newsgroup postings, pop-up or pop-under Internet advertising or fax-blasting, direct mailing or telemarketing, or claims alleging violations of the Telephone Consumer Protection Act, of 1991, as amended, the CAN-SPAM Act of 2003, as amended, and any other federal, foreign or state anti-spam statutes, or federal, foreign or state statute, law or regulation relating to a person's right to seclusion and privacy.
- o. Any uploading, downloading, piracy or file-sharing of digitized music, photos, movies, software or video games.
- p. Any actual or alleged:
 - (1) Price fixing, restraint of trade, monopolization, including violations of the Sherman Anti-Trust Act, the Clayton Act, or any similar provision of any federal, state, or local statutory law or common law anywhere in the world; or
 - (2) Unfair trade practices or violation of consumer protection laws; provided, however that this exclusion does not apply to any otherwise covered claim under Insuring Agreements E or F; or
 - (3) Violation of the Employee Retirement Income Security Act of 1974, as amended; the Securities Act of 1933, as amended; the Securities Exchange Act of 1934 as amended; or any state Blue Sky or securities law or similar state, foreign or federal statute, including any regulation or order issued pursuant to any of the foregoing statutes.
- q. Any actual or alleged infringement, misappropriation or violation of any patent, copyright, trademark, service mark, trade dress or trade name.
- r. Alleging, based upon, arising out of, or resulting from, directly or indirectly, to section 605 (requirements relating to information contained in consumer reports) or 616 (civil liability for willful noncompliance) of the Fair Credit Reporting Act, or any other similar federal, state or local laws or regulations, including but not limited to any laws or regulations requiring truncation of payment card numbers on, or the removal of the expiration date from, payment card receipts.

4. Extended Reporting Periods

- a. We will provide one or more Extended Reporting Periods, as described below, and notify you in writing within thirty days of policy termination, if:
 - (1) This Coverage Part is canceled or not renewed; or
 - (2) We renew or replace this endorsement with other insurance that does not apply to monetary damages on a first discovered and reported basis; or
 - (3) We renew or replace this endorsement with other insurance containing terms and conditions that are less favorable for you than those contained in this endorsement.
- b. Extended Reporting Periods do not extend the policy period or change the scope of coverage provided. They only apply to claims arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period. Once in effect, Extended Reporting Periods may not be canceled.
- c.
 - (1) A Basic Extended Reporting Period is automatically provided without additional charge. This period starts with the end of the policy period and lasts for sixty (60) days.
 - (2) During the Basic Extended Reporting Period you have the right to report claims made against you arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period, or to report any "network security or data breach event" or "privacy event" that occurred prior to the end of the policy period which may later result in a claim or "privacy event mitigation expenses".
 - (3) The Basic Extended Reporting Period does not apply to any claims or "privacy event mitigation expenses" that are covered under any subsequent insurance you purchase, or that would be covered but for exhaustion of the amount of insurance applicable to such claims or "privacy event mitigation expenses".
 - (4) The Basic Extended Reporting Period does not reinstate or increase the Limits of Insurance.

- d. (1) A Supplemental Extended Reporting Period of five (5) years duration is available, but only by an endorsement and for an extra charge. This supplemental period starts when the Basic Extended Reporting Period, set forth in c. above, ends.
- (2) During the Supplemental Extended Reporting Period you will have the right to report claims made against you arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period, or to report any "network security or data breach event" or "privacy event" that occurred prior to the end of the policy period which may later result in a claim or "privacy event mitigation expenses". There is no coverage during the Supplemental Extended Reporting Period for any other claims or "privacy event mitigation expenses".
- (3) You must give us a written request for the endorsement within sixty (60) days after the end of the policy period. The Supplemental Extended Reporting Period will not go into effect unless you pay the additional premium promptly when due.
- (4) We will determine the additional premium in accordance with our rules and rates in effect on the date the policy was issued or last renewed. In doing so, we may take into account the following:
- (a) The exposure insured;
 - (b) Previous types and amounts of insurance;
 - (c) Limits of insurance available under this endorsement for future payments and damages; and
 - (d) Other related factors.

The additional premium will not exceed 200% of the expiring annual premium for this coverage.

- (5) This endorsement shall set forth the terms, not inconsistent with this section, applicable to the Supplemental Extended Reporting Period, including a provision to the effect that the insurance afforded for claims and "privacy event mitigation expenses" first discovered during such period is excess over any other valid and collectible insurance available under policies in force after the Supplemental Extended Reporting Period starts.
- e. If the Supplemental Extended Reporting Period is in effect, we will provide Supplemental Aggregate Limits of Insurance as described below, but only for claims arising out of "network security or data breach events" or "privacy event mitigation expenses" arising out of "privacy events" which are first discovered during the Supplemental Extended Reporting Period. Paragraph 2. of **Section III – Limits Of Insurance** will be amended to include the following:
- (1) Claims arising out of "network security or data breach events" first discovered during the Supplemental Extended Reporting Period will be subject to a Supplemental Aggregate Limit equal to the dollar amount shown in the Schedule for the Network Security or Data Breach Liability Aggregate Limit in effect at the end of the policy period. The Supplemental Aggregate Limit is the most we will pay for the sum of all monetary damages under **Coverage E – Network Security or Data Breach Liability** arising out of claims first discovered during the Supplemental Extended Reporting Period. If we make a payment for such monetary damages, the Supplemental Aggregate Limit will be reduced by the amount of such payment. Such reduced limit will then be the amount available for further covered monetary damages arising out of "network security or data breach events" first discovered during the Supplemental Extended Reporting Period. The Network Security or Data Beach Liability Each Event Limit will continue to apply.
- (2) "Privacy event mitigation expenses" arising out of "privacy events" first discovered during the Supplemental Extended Reporting Period will be subject to a Supplemental Aggregate Limit equal to the dollar amount shown in the Schedule for the Privacy Event Mitigation Expense Aggregate Limit in effect at the end of the policy period. The Supplemental Aggregate Limit is the most we will pay for the sum of all "privacy event mitigation expenses" under **Coverage F – Privacy Event Mitigation Expense** arising out of "privacy events" first discovered during the Supplemental Extended Reporting Period. If we make a payment for such "privacy event mitigation expenses", the Supplemental Aggregate Limit will be reduced by the amount of such payment. Such reduced limit will then be the amount available for further covered "privacy events" first discovered during the Supplemental Extended Reporting Period. The Privacy Event Mitigation Expense Each Event Limit will continue to apply.

B. Supplementary Payments Coverages A and B is amended to read:

Supplementary Payments – Coverages A, B and E.

C. Limits Of Insurance

For the purposes of coverage provided by this endorsement, the following is added to **Section III – Limits Of Insurance**:

1. The Limits of Insurance shown in the Schedule and the rules below fix the most we will pay regardless of the number of:
 - a. Insureds;
 - b. Claims made, "suits" brought or "privacy events"; or
 - c. Persons or organizations making claims or bringing "suits."
2. The following applies to **Coverage E – Network Security or Data Breach Liability**:
 - a. The Network Security or Data Breach Liability Aggregate Limit shown in the Schedule is the most we will pay for the sum of all monetary damages under this endorsement;
 - b. Subject to **2.a.** above, the Network Security or Data Breach Liability Each Event Limit is the most we will pay for all monetary damages resulting from any one "network security or data breach event". All monetary damages arising out of related "network security or data breach events" will be deemed to be one "network security or data breach event".
3. The following applies to **Coverage F – Privacy Event Mitigation Expense**:
 - a. The Privacy Event Mitigation Expense Aggregate Limit shown in the Schedule is the most we will pay for the sum of all "privacy event mitigation expenses" under this endorsement;
 - b. Subject to **3.a.** above, the Privacy Event Mitigation Expense Each Event Limit is the most we will pay for all "privacy event mitigation expenses" resulting from any one "privacy event". All "privacy event mitigation expenses" arising out of related "privacy events" will be deemed to be one "privacy event".
4. The Limits of Insurance under this endorsement apply separately to each consecutive annual period and to any remaining period of less than 12 months, starting with the beginning of the policy period shown in the Declarations, unless the policy period is extended after issuance for an additional period of less than 12 months. In that case, the additional period will be deemed part of the last preceding period for purposes of determining the limits of insurance.

D. Conditions

For the purposes of coverage provided by this endorsement, **Section IV – Conditions** is modified as follows:

1. Sub-paragraph **a.** under Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit** as respects coverage provided by **Coverage E – Network Security or Data Breach Liability** is deleted and replaced by the following:
 - a. You must see to it that we are notified as soon as practicable of a "network security or data breach event," "occurrence" or an offense which may result in a claim or "suit." To the extent possible, notice should include:
 - (1) How, when and where the "network security or data breach event," "occurrence" or offense took place;
 - (2) The names and addresses of any injured persons and witnesses; and
 - (3) The nature and location of any injury or damage arising out of the "network security or data breach event," "occurrence" or offense.
2. The following is added under Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit** as respects coverage provided by **Coverage F – Privacy Event Mitigation Expense**:
 - e. You must cooperate with us and our designated representatives in the provision of the services described in "privacy event mitigation expenses".
3. The following is added as respects coverage provided by **Coverage F – Privacy Event Mitigation Expense**:

Duties in the Event of a Privacy Event

 - a. You must notify us as soon as practicable of a "privacy event", but in no event later than thirty (30) days after you incur "privacy event mitigation expenses" for which coverage will be requested under this endorsement.
 - b. With respect to a "privacy event", you must notify us in writing as soon as practicable but no later than sixty (60) days after the first discovery of the "privacy event" by you. Notice must include:
 - (1) How, when and where the "privacy event" took place;
 - (2) A description of the "privacy event";
 - (3) The number of individuals and type of "personally identifiable information" involved in the "privacy event";

- (4) Upon request by us, the names and addresses of individuals affected by the "privacy event".
- c. You must provide us with all information and assistance that we request and cooperate with us and our designated representatives in the:
 - (1) Investigation of any "privacy event" or any acts, errors or omissions that may result in a "privacy event"; and
 - (2) Provision of the services described in "privacy event mitigation expenses".

4. The following is added as respects coverage provided by this endorsement:

Your Right to Claim Information

- a. Upon request, we will provide the first Named Insured shown in the Declarations the following information relating to this and any preceding first discovery coverage endorsement we have issued to you during the previous three years:
 - (1) A list or other record of each "network security or data breach event" or "privacy event", not previously reported to any other insurer, of which we were notified in accordance with Paragraph 2. **Duties In the Event of Occurrence, Offence, Claim or Suit of Section IV – Conditions** or Paragraph D.3. above. We will include the date and brief description of the "network security or data breach event" or "privacy event" if that information was in the notice we received.
 - (2) A summary by policy year, of payments made and amounts reserved, stated separately, under any applicable aggregate limit.
Amounts reserved are based on our judgment. They are subject to change and should not be regarded as ultimate settlement values.
- b. You must not disclose this information to any claimant or any claimant's representative without our consent.
- c. We compile claim and related information for our own business purposes and exercise reasonable care in doing so. In providing this information to the first Named Insured, we make no representations or warranties to insureds, insurers, or others to whom this information is furnished by or on behalf of any insured. Cancellation or non-renewal will be effective even if we inadvertently provide inaccurate information.

5. All references to **Coverages A** and **B** are amended to read **Coverages A, B, E, and F** under Paragraph 4. **Other Insurance** as respects coverage provided by this endorsement.

6. The following is added under Paragraph 4. **Other Insurance** as respects coverage provided by this endorsement:

- d. However, if the insured has another policy, coverage part or endorsement issued by us or one of our affiliated companies that applies to damages, loss or expense we cover under this endorsement, the most we will pay in total is the single largest applicable limit. This limitation on the amount we will pay applies regardless of whether this coverage or the other coverage is primary, unless the other coverage was purchased specifically to apply in excess of this coverage.

E. The following definitions are added to **Section V – Definitions**:

- 1. "Computer system" means any:
 - a. Computer hardware, including Personal Digital Assistants (PDAs) and other transportable or hand held devices, software or firmware, or components thereof including data stored thereon, and associated networking equipment or backup facilities;
 - b. Communications networks including the internet, intranets, extranets or virtual private networks to the extent used by the items in a. above;By which "electronic data" is collected, transmitted, processed, stored or retrieved.
"Computer system" includes "electronic data" that is stored on any of the items described in a. above or temporarily outside of your "computer system" for use by an insured.
- 2. "Confidential corporate information" means any commercial trade secret, data, design, interpretation, forecast, formula, method, practice, process, record, report or other item of information of a third party which is:
 - a. Not available to the general public; and
 - (1) Provided to you under a mutually agreed to written confidentiality or non-disclosure agreement; or
 - (2) Marked confidential or otherwise specifically designated in writing as confidential by such third party.

3. "Electronic Data" means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.
4. "Network Security or Data Breach Event" means:
 - a. Transmission of malware from your "computer system" to a third party;
 - b. The inability of an authorized user to access your website or your "computer system" because of a denial of service attack; or
 - c. A "privacy event".

As used in this definition, a denial of service attack means a malicious attack intended by the perpetrator to overwhelm the capacity of your "computer system" or website by sending an excessive volume of "electronic data" to such "computer system" or website in order to prevent authorized access to it.

5. "Personally identifiable information" means any:
 - a. Individual's name in combination with any one or more of the following:
 - (1) Social security number;
 - (2) Drivers license number or any other state identification number;
 - (3) Medical or healthcare data including protected health information;
 - (4) Any account number, credit card number or debit card number;
 - (5) Any account relationships, account balances or account histories; or
 - (6) Any password, access code or other security code that would permit access to a financial account.
 - b. Non-public personal information as defined in any part of the following statutes or regulations which regulate the use and protection of non-public personal information (as defined in such statutes or regulations):
 - (1) Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the rules and regulations promulgated thereunder, as amended;
 - (2) Gramm-Leach Bliley Act of 1999 (GLBA) and the rules and regulations promulgated thereunder, as amended; or
 - (3) Other state, federal or local privacy laws requiring reasonable security within a "computer system" for non-public personal information, or a privacy policy limiting the sale, disclosure or sharing of non-public personal information or providing individuals with the right to access or collect non-public personal information.
6. "Privacy Event" means:
 - a. Unauthorized disclosure of, loss of, theft of, or unintentional delivery or exposure to others of "personally identifiable information" or "confidential corporate information" which is in the insured's care, custody or control. Such disclosure, loss, theft or unintentional delivery or exposure to others is limited to information obtained or released directly from your "computer system"; or
 - b. Failure by you to disclose or warn of actual or potential disclosure or misappropriation of "personally identifiable information" or "confidential corporate information", but only if this endorsement covers such disclosure or misappropriation and it resulted directly from **a.** above; or
 - c. Violation or the investigation of a violation of any federal, state or local privacy statute addressing disclosure or misappropriation of "personally identifiable information" or "confidential corporate information", but only if this endorsement covers such disclosure or misappropriation and it resulted directly from **a.** above.
7. "Privacy Event Mitigation Expense" means:
 - a. Reasonable and necessary fees and expenses for:
 - (1) An outside vendor to conduct a computer forensic analysis with reasonable allocation of time and resources to investigate your "computer system" to determine the cause and extent of a "privacy event";
 - (2) An approved crisis management or legal firm to review the "privacy event" and advise you on the appropriate response;
 - (3) Travel by directors, executive officers, partners or employees of the insured which is done to mitigate damage from the "privacy event";
 - (4) Printing, advertising, mailing of materials or other costs to provide notice to affected parties of a "privacy event" for the purposes of maintaining good will or compliance with any notification requirements imposed by law; and

- (5)** Services provided to any individual whose primary identification is the subject of a “privacy event”, but only if the primary purpose of such services is mitigating the effect of the “privacy event”:
 - (i)** Reasonable fees and expenses to establish, maintain and provide call center services;
 - (ii)** Credit file monitoring services; or
 - (iii)** Reasonable fees and expenses for any other service specifically approved by us in writing.
- b.** However, “privacy event mitigation expense” shall not include:
 - (1)** Compensation, fees, benefits or overhead of any insured or employee of any insured;
 - (2)** Costs or expenses that would have been incurred in the absence of the “privacy event”;
 - (3)** Costs or expenses associated with upgrading, maintaining, improving, repairing or remediating any “computer system” as a result of a “privacy event”; or
 - (4)** Costs or expenses associated with upgrading, maintaining, improving, repairing or remediating any procedures, services or property as a result of a “privacy event”.

State: District of Columbia **Filing Company:** Arch Insurance Company
TOI/Sub-TOI: 17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability
Product Name: Network Security and Data Breach Endorsement Revision
Project Name/Number: ESIP General Liability Form Revision/ARCH-16-177

Supporting Document Schedules

Satisfied - Item:	Readability Certificate
Comments:	Acknowledged
Attachment(s):	
Item Status:	
Status Date:	

Bypassed - Item:	Consulting Authorization
Bypass Reason:	Not Applicable
Attachment(s):	
Item Status:	
Status Date:	

Bypassed - Item:	Copy of Trust Agreement
Bypass Reason:	Not Applicable
Attachment(s):	
Item Status:	
Status Date:	

Bypassed - Item:	Expedited SERFF Filing Transmittal Form
Bypass Reason:	Not Applicable
Attachment(s):	
Item Status:	
Status Date:	

Satisfied - Item:	Cover Letter
Comments:	Please see attached file.
Attachment(s):	ARCH-16-177 Cover Letter.pdf
Item Status:	
Status Date:	

Satisfied - Item:	Red-Lined
Comments:	Please see attached file.
Attachment(s):	GL 4000 10 16-Network Security and Data Breach (REDLINED).pdf
Item Status:	
Status Date:	

SERFF Tracking #:

AICO-130810784

State Tracking #:

Company Tracking #:

ARCH-16-177

State:

District of Columbia

Filing Company:

Arch Insurance Company

TOI/Sub-TOI:

17.0 Other Liability-Occ/Claims Made/17.0001 Commercial General Liability

Product Name:

Network Security and Data Breach Endorsement Revision

Project Name/Number:

ESIP General Liability Form Revision/ARCH-16-177



Arch Insurance Company

Harborside 3
210 Hudson Street, Suite 300
Jersey City, NJ 07311

T: 201.743.4000

F: 201.743.4005

archinsurance.com

November 16, 2016

Department of Insurance
Property and Casualty Division
Form Review Section

RE: Arch Insurance Company – NAIC - #: 1279-11150
ESIP General Liability Form Filing
Revised Form Filing
Company Filing Number: ARCH-16-177

To Whom It May Concern:

Arch Insurance Company (Arch) is submitting for your review and approval a revised General Liability form filing for use with its Emergency Services Insurance Program (ESIP) in your state.

Form GL 4000 is an optional endorsement selected at the request of the insured. It provides network security and data breach coverage for events first discovered during the policy period or any extended reporting period.

We are revising exclusion 'k' in order to clarify our intent to give back coverage for an insured to be able to file suit against a named insured specifically for a privacy event.

Enclosed for your review is:
GL 4000 10 16 – Network Security and Data Breach

A marked up version of the revised form has been provided to show the proposed change.

There is no rate impact associated with this form.

Sincerely,

Tara Martin

Tara Martin

Compliance Analyst

ARCH INSURANCE COMPANY

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

NETWORK SECURITY AND DATA BREACH ENDORSEMENT

Insured:	Policy No.:	Effective Date:
----------	-------------	-----------------

NOTICE: EXCEPT AS OTHERWISE PROVIDED, THE COVERAGE PROVIDED BY THIS ENDORSEMENT IS LIMITED TO ONLY THOSE EVENTS THAT ARE FIRST DISCOVERED AND REPORTED WHILE THIS POLICY IS IN FORCE OR DURING ANY EXTENDED REPORTING PERIOD. VARIOUS PROVISIONS IN THIS ENDORSEMENT RESTRICT COVERAGE. PLEASE READ THE ENTIRE ENDORSEMENT CAREFULLY TO DETERMINE RIGHTS, DUTIES AND WHAT IS AND IS NOT COVERED.

This endorsement modifies the insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE FORM

SCHEDULE

Coverage E – Network Security and Data Breach Liability

Network Security and Data Breach Liability Each Event Limit	\$
Network Security and Data Breach Liability Aggregate Limit	\$
Network Security and Data Breach Liability Retroactive Date	

Coverage F – Privacy Event Mitigation Expense

Privacy Event Mitigation Expense Each Event Limit	\$
Privacy Event Mitigation Expense Aggregate Limit	\$
Privacy Event Mitigation Expense Retroactive Date	

A. The following are added to **Section I – Coverages**:

1. Coverage E – Network Security and Data Breach Liability

Insuring Agreement

a. We will pay those sums that the insured becomes legally obligated to pay as monetary damages because of a "network security or data breach event" to which this insurance applies. We have the right and duty to defend the insured against any "suit" seeking those monetary damages. We have no duty to defend the insured against any "suit" not seeking monetary damages. We also have no duty to defend the insured against any "suit" based upon, arising out of, or attributable to a "network security or data breach event" to which this insurance does not apply. However, at our discretion, we have the right to investigate any "network security or data breach event" and settle any claim or "suit" that may result. But:

(1) The amount we will pay for monetary damages is limited as described below in **Section C. Limits Of Insurance**;

(2) Our right and duty to defend ends when we have used up the applicable limit of insurance in the payment of judgments or settlements.

No other obligation or liability to pay sums or perform acts or services is covered unless explicitly provided for under **Supplementary Payments – Coverages A, B and E**.

b. This insurance applies to a "network security or data breach event" only if:

(1) Such "network security or data breach event" takes place in the "coverage territory"; and

(2) Such "network security or data breach event" did not result from an act, error or omission that occurred before the Network Security and Data Breach Liability Retroactive Date shown in the schedule or after the end of the policy period; and

- (3) The "network security or data breach event" is first discovered in accordance with Paragraph c. below during the policy period or any Extended Reporting Period we provide under **4. Extended Reporting Periods**; and
- (4) Written notice is received by us of the "network security or data breach event" within sixty (60) days of its first discovery or before the end of any Extended Reporting Period we provide under **4. Extended Reporting Periods**, whichever is earlier.

c. First Discovery and Related Events or Acts

(1) First Discovery

A "network security or data breach event" will be deemed to have been discovered at the earliest of the following times:

- (a) When such "network security or data breach event" is discovered and recorded by any insured, or by us, whichever comes first; or
- (b) When the insured becomes aware of an act, error or omission that may subsequently result in a "network security or data breach event", and you give written notice to us, as described in **Section IV – Conditions**, of such circumstances as soon as practicable but no later than:
 - (i) Sixty (60) days after becoming aware; or
 - (ii) The end of any applicable Extended Reporting Period; whichever is earlier.

(2) Related Events

All related "network security or data breach events" will be considered one event and will be considered first discovered when the first of such related events is discovered.

Related "network security or data breach events" include all "network security or data breach events" that are logically or causally connected by a common nexus of facts, circumstances, situations, events, transactions, causes or acts.

2. Coverage F – Privacy Event Mitigation Expense

Insuring Agreement

- a. We will pay "privacy event mitigation expenses" incurred by the insured, provided such expenses arise directly out of a "privacy event" for which coverage is not otherwise excluded. But the amount we will pay is limited as described below in **Section C – Limits Of Insurance**;

No other obligation or liability to pay sums or perform acts or services is covered.

- b. This insurance applies to "privacy event mitigation expenses" only if:

- (1) The "privacy event" takes place in the "coverage territory"; and
- (2) The "privacy event" did not result from an act, error or omission that occurred before the Privacy Event Mitigation Expense Retroactive Date shown in the schedule or after the end of the policy period; and
- (3) The "privacy event" is first discovered in accordance with Paragraph c. below during the policy period or any Extended Reporting Period we provide under **4. Extended Reporting Periods**; and
- (4) Written notice is received by us of the "privacy event" within sixty (60) days of its first discovery or before the end of any Extended Reporting Period we provide under **4. Extended Reporting Periods**, whichever is earlier.

c. First Discovery and Related Events or Acts

(1) First Discovery

A "privacy event" will be deemed to have been discovered at the earliest of the following times:

- (a) When such "privacy event" is discovered and recorded by any insured, or by us, whichever comes first; or
- (b) When you become aware of an act, error or omission that may subsequently result in a "privacy event", and you give written notice to us, as described in **Section IV – Conditions**, of such circumstances as soon as practicable but no later than:
 - (i) Sixty (60) days after becoming aware; or
 - (ii) The end of any applicable Extended Reporting Period; whichever is earlier.

(2) Related Events

All related "privacy events" will be considered one event and will be considered first discovered when the first of such related events is discovered.

Related "privacy events" include all "privacy events" that are the same, related or continuous, or that arise from a common nucleus of facts, circumstances, events or acts.

3. Exclusions

This insurance does not apply to:

- a. Damages, loss or expense arising directly or indirectly from:
 - (1) Any shortcoming in data security that the insured knew about prior to the inception of this policy for which you failed to take corrective action within a reasonable time, not to exceed sixty (60) days;
 - (2) The insured's failure to comply with all the data security standards issued by credit card issuers or financial institutions with whom you transact business, if you process, store or handle credit card information;
 - (3) The insured's failure to take reasonable steps to use, design, maintain and upgrade your data security; or
 - (4) The inability to use or lack of performance of software:
 - (a) Due to expiration, cancellation or withdrawal of such software;
 - (b) That has not yet been released from its development stage; or
 - (c) That has not passed all test runs or proven successful in applicable daily operations.
- b. Damages, loss or expense arising directly or indirectly from:
 - (1) The illegal, unauthorized or wrongful collection of "personally identifiable information" including but not limited to collection of "personally identifiable information" using cookies or malware, if committed by or with the knowledge of the insured; or
 - (2) The failure to provide required notice that such "personally identifiable information" is being collected.
- c. Damages, loss or expense arising directly or indirectly from the seizure, confiscation, expropriation, nationalization or destruction of a "computer system" by order of any governmental authority.
- d. Any "network security or data breach event" or "privacy event" that results from an act, error or omission that takes place prior to the inception date of this policy if the insured knew or reasonably should have foreseen that such act, error or omission would give rise to a claim or "privacy event mitigation expense".
- e. Damages, loss or expense based upon, attributable to, arising out of, in consequence of, or in any way related to litigation or any administrative or regulatory proceedings if such litigation or administrative or regulatory proceedings were initiated prior to or were pending on the inception date of this policy.
- f. "Bodily injury", "property damage" or "personal and advertising injury".
- g. Violation or invasion of any right of privacy except as a result of a "privacy event".
- h. Breach of contract by an insured or liability assumed by an insured under any contract or agreement. This exclusion does not apply to liability the insured would have in the absence of the contract or agreement.
- i. Fines or penalties imposed by any federal, state or local governmental authority.
- j. Any fraudulent, dishonest, malicious, or criminal act by the insured.
- k. ~~Any claim or "suit" for "damages" made against any insured that is brought by or on behalf of any other insured.~~ Any "claim" or "suit" brought by or on behalf of any insured against any other insured; provided, however, that this exclusion will not apply to any otherwise covered "claim" or "suit" brought by or on behalf of any insured against a Named Insured arising out of a "privacy event", provided that such insured is not involved in any manner with any such "privacy event".
- l. Costs or expenses incurred by the insured to comply with any demand or order by any federal, state or local governmental authority other than those provided under **Coverage F – Privacy Event Mitigation Expense**.
- m. Any cost to comply with any injunctive or other non-monetary or declaratory relief or any agreement to provide such relief.

- n. Any claim or "suit" alleging, based upon, arising out of, or resulting from, directly or indirectly, any unsolicited electronic faxes, emails, telephone calls or unsolicited communications, including but not limited to claims arising out of unsolicited electronic messages, chat room postings, bulletin board postings, newsgroup postings, pop-up or pop-under Internet advertising or fax-blasting, direct mailing or telemarketing, or claims alleging violations of the Telephone Consumer Protection Act, of 1991, as amended, the CAN-SPAM Act of 2003, as amended, and any other federal, foreign or state anti-spam statutes, or federal, foreign or state statute, law or regulation relating to a person's right to seclusion and privacy.
- o. Any uploading, downloading, piracy or file-sharing of digitized music, photos, movies, software or video games.
- p. Any actual or alleged:
 - (1) Price fixing, restraint of trade, monopolization, including violations of the Sherman Anti-Trust Act, the Clayton Act, or any similar provision of any federal, state, or local statutory law or common law anywhere in the world; or
 - (2) Unfair trade practices or violation of consumer protection laws; provided, however that this exclusion does not apply to any otherwise covered claim under Insuring Agreements E or F; or
 - (3) Violation of the Employee Retirement Income Security Act of 1974, as amended; the Securities Act of 1933, as amended; the Securities Exchange Act of 1934 as amended; or any state Blue Sky or securities law or similar state, foreign or federal statute, including any regulation or order issued pursuant to any of the foregoing statutes.
- q. Any actual or alleged infringement, misappropriation or violation of any patent, copyright, trademark, service mark, trade dress or trade name.
- r. Alleging, based upon, arising out of, or resulting from, directly or indirectly, to section 605 (requirements relating to information contained in consumer reports) or 616 (civil liability for willful noncompliance) of the Fair Credit Reporting Act, or any other similar federal, state or local laws or regulations, including but not limited to any laws or regulations requiring truncation of payment card numbers on, or the removal of the expiration date from, payment card receipts.

4. Extended Reporting Periods

- a. We will provide one or more Extended Reporting Periods, as described below, and notify you in writing within thirty days of policy termination, if:
 - (1) This Coverage Part is canceled or not renewed; or
 - (2) We renew or replace this endorsement with other insurance that does not apply to monetary damages on a first discovered and reported basis; or
 - (3) We renew or replace this endorsement with other insurance containing terms and conditions that are less favorable for you than those contained in this endorsement.
- b. Extended Reporting Periods do not extend the policy period or change the scope of coverage provided. They only apply to claims arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period. Once in effect, Extended Reporting Periods may not be canceled.
- c.
 - (1) A Basic Extended Reporting Period is automatically provided without additional charge. This period starts with the end of the policy period and lasts for sixty (60) days.
 - (2) During the Basic Extended Reporting Period you have the right to report claims made against you arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period, or to report any "network security or data breach event" or "privacy event" that occurred prior to the end of the policy period which may later result in a claim or "privacy event mitigation expenses".
 - (3) The Basic Extended Reporting Period does not apply to any claims or "privacy event mitigation expenses" that are covered under any subsequent insurance you purchase, or that would be covered but for exhaustion of the amount of insurance applicable to such claims or "privacy event mitigation expenses".
 - (4) The Basic Extended Reporting Period does not reinstate or increase the Limits of Insurance.

- d. (1) A Supplemental Extended Reporting Period of five (5) years duration is available, but only by an endorsement and for an extra charge. This supplemental period starts when the Basic Extended Reporting Period, set forth in c. above, ends.
- (2) During the Supplemental Extended Reporting Period you will have the right to report claims made against you arising out of "network security or data breach event" or "privacy event mitigation expenses" arising out of a "privacy event" that occurred prior to the end of the policy period, or to report any "network security or data breach event" or "privacy event" that occurred prior to the end of the policy period which may later result in a claim or "privacy event mitigation expenses". There is no coverage during the Supplemental Extended Reporting Period for any other claims or "privacy event mitigation expenses".
- (3) You must give us a written request for the endorsement within sixty (60) days after the end of the policy period. The Supplemental Extended Reporting Period will not go into effect unless you pay the additional premium promptly when due.
- (4) We will determine the additional premium in accordance with our rules and rates in effect on the date the policy was issued or last renewed. In doing so, we may take into account the following:
- (a) The exposure insured;
 - (b) Previous types and amounts of insurance;
 - (c) Limits of insurance available under this endorsement for future payments and damages; and
 - (d) Other related factors.

The additional premium will not exceed 200% of the expiring annual premium for this coverage.

- (5) This endorsement shall set forth the terms, not inconsistent with this section, applicable to the Supplemental Extended Reporting Period, including a provision to the effect that the insurance afforded for claims and "privacy event mitigation expenses" first discovered during such period is excess over any other valid and collectible insurance available under policies in force after the Supplemental Extended Reporting Period starts.
- e. If the Supplemental Extended Reporting Period is in effect, we will provide Supplemental Aggregate Limits of Insurance as described below, but only for claims arising out of "network security or data breach events" or "privacy event mitigation expenses" arising out of "privacy events" which are first discovered during the Supplemental Extended Reporting Period. Paragraph 2. of **Section III – Limits Of Insurance** will be amended to include the following:
- (1) Claims arising out of "network security or data breach events" first discovered during the Supplemental Extended Reporting Period will be subject to a Supplemental Aggregate Limit equal to the dollar amount shown in the Schedule for the Network Security or Data Breach Liability Aggregate Limit in effect at the end of the policy period. The Supplemental Aggregate Limit is the most we will pay for the sum of all monetary damages under **Coverage E – Network Security or Data Breach Liability** arising out of claims first discovered during the Supplemental Extended Reporting Period. If we make a payment for such monetary damages, the Supplemental Aggregate Limit will be reduced by the amount of such payment. Such reduced limit will then be the amount available for further covered monetary damages arising out of "network security or data breach events" first discovered during the Supplemental Extended Reporting Period. The Network Security or Data Beach Liability Each Event Limit will continue to apply.
- (2) "Privacy event mitigation expenses" arising out of "privacy events" first discovered during the Supplemental Extended Reporting Period will be subject to a Supplemental Aggregate Limit equal to the dollar amount shown in the Schedule for the Privacy Event Mitigation Expense Aggregate Limit in effect at the end of the policy period. The Supplemental Aggregate Limit is the most we will pay for the sum of all "privacy event mitigation expenses" under **Coverage F – Privacy Event Mitigation Expense** arising out of "privacy events" first discovered during the Supplemental Extended Reporting Period. If we make a payment for such "privacy event mitigation expenses", the Supplemental Aggregate Limit will be reduced by the amount of such payment. Such reduced limit will then be the amount available for further covered "privacy events" first discovered during the Supplemental Extended Reporting Period. The Privacy Event Mitigation Expense Each Event Limit will continue to apply.

B. Supplementary Payments Coverages A and B is amended to read:

Supplementary Payments – Coverages A, B and E.

C. Limits Of Insurance

For the purposes of coverage provided by this endorsement, the following is added to **Section III – Limits Of Insurance**:

1. The Limits of Insurance shown in the Schedule and the rules below fix the most we will pay regardless of the number of:
 - a. Insureds;
 - b. Claims made, "suits" brought or "privacy events"; or
 - c. Persons or organizations making claims or bringing "suits."
2. The following applies to **Coverage E – Network Security or Data Breach Liability**:
 - a. The Network Security or Data Breach Liability Aggregate Limit shown in the Schedule is the most we will pay for the sum of all monetary damages under this endorsement;
 - b. Subject to **2.a.** above, the Network Security or Data Breach Liability Each Event Limit is the most we will pay for all monetary damages resulting from any one "network security or data breach event". All monetary damages arising out of related "network security or data breach events" will be deemed to be one "network security or data breach event".
3. The following applies to **Coverage F – Privacy Event Mitigation Expense**:
 - a. The Privacy Event Mitigation Expense Aggregate Limit shown in the Schedule is the most we will pay for the sum of all "privacy event mitigation expenses" under this endorsement;
 - b. Subject to **3.a.** above, the Privacy Event Mitigation Expense Each Event Limit is the most we will pay for all "privacy event mitigation expenses" resulting from any one "privacy event". All "privacy event mitigation expenses" arising out of related "privacy events" will be deemed to be one "privacy event".
4. The Limits of Insurance under this endorsement apply separately to each consecutive annual period and to any remaining period of less than 12 months, starting with the beginning of the policy period shown in the Declarations, unless the policy period is extended after issuance for an additional period of less than 12 months. In that case, the additional period will be deemed part of the last preceding period for purposes of determining the limits of insurance.

D. Conditions

For the purposes of coverage provided by this endorsement, **Section IV – Conditions** is modified as follows:

1. Sub-paragraph **a.** under Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit** as respects coverage provided by **Coverage E – Network Security or Data Breach Liability** is deleted and replaced by the following:
 - a. You must see to it that we are notified as soon as practicable of a "network security or data breach event," "occurrence" or an offense which may result in a claim or "suit." To the extent possible, notice should include:
 - (1) How, when and where the "network security or data breach event," "occurrence" or offense took place;
 - (2) The names and addresses of any injured persons and witnesses; and
 - (3) The nature and location of any injury or damage arising out of the "network security or data breach event," "occurrence" or offense.
2. The following is added under Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit** as respects coverage provided by **Coverage F – Privacy Event Mitigation Expense**:
 - e. You must cooperate with us and our designated representatives in the provision of the services described in "privacy event mitigation expenses".
3. The following is added as respects coverage provided by **Coverage F – Privacy Event Mitigation Expense**:

Duties in the Event of a Privacy Event

 - a. You must notify us as soon as practicable of a "privacy event", but in no event later than thirty (30) days after you incur "privacy event mitigation expenses" for which coverage will be requested under this endorsement.
 - b. With respect to a "privacy event", you must notify us in writing as soon as practicable but no later than sixty (60) days after the first discovery of the "privacy event" by you. Notice must include:
 - (1) How, when and where the "privacy event" took place;
 - (2) A description of the "privacy event";
 - (3) The number of individuals and type of "personally identifiable information" involved in the "privacy event";

- (4) Upon request by us, the names and addresses of individuals affected by the “privacy event”.
- c. You must provide us with all information and assistance that we request and cooperate with us and our designated representatives in the:
 - (1) Investigation of any “privacy event” or any acts, errors or omissions that may result in a “privacy event”; and
 - (2) Provision of the services described in “privacy event mitigation expenses”.

4. The following is added as respects coverage provided by this endorsement:

Your Right to Claim Information

- a. Upon request, we will provide the first Named Insured shown in the Declarations the following information relating to this and any preceding first discovery coverage endorsement we have issued to you during the previous three years:
 - (1) A list or other record of each "network security or data breach event" or "privacy event", not previously reported to any other insurer, of which we were notified in accordance with Paragraph 2. **Duties In the Event of Occurrence, Offence, Claim or Suit of Section IV – Conditions** or Paragraph D.3. above. We will include the date and brief description of the "network security or data breach event" or "privacy event" if that information was in the notice we received.
 - (2) A summary by policy year, of payments made and amounts reserved, stated separately, under any applicable aggregate limit.
Amounts reserved are based on our judgment. They are subject to change and should not be regarded as ultimate settlement values.
- b. You must not disclose this information to any claimant or any claimant's representative without our consent.
- c. We compile claim and related information for our own business purposes and exercise reasonable care in doing so. In providing this information to the first Named Insured, we make no representations or warranties to insureds, insurers, or others to whom this information is furnished by or on behalf of any insured. Cancellation or non-renewal will be effective even if we inadvertently provide inaccurate information.

5. All references to **Coverages A** and **B** are amended to read **Coverages A, B, E, and F** under Paragraph 4. **Other Insurance** as respects coverage provided by this endorsement.

6. The following is added under Paragraph 4. **Other Insurance** as respects coverage provided by this endorsement:

- d. However, if the insured has another policy, coverage part or endorsement issued by us or one of our affiliated companies that applies to damages, loss or expense we cover under this endorsement, the most we will pay in total is the single largest applicable limit. This limitation on the amount we will pay applies regardless of whether this coverage or the other coverage is primary, unless the other coverage was purchased specifically to apply in excess of this coverage.

E. The following definitions are added to **Section V – Definitions**:

- 1. “Computer system” means any:
 - a. Computer hardware, including Personal Digital Assistants (PDAs) and other transportable or hand held devices, software or firmware, or components thereof including data stored thereon, and associated networking equipment or backup facilities;
 - b. Communications networks including the internet, intranets, extranets or virtual private networks to the extent used by the items in a. above;
 By which “electronic data” is collected, transmitted, processed, stored or retrieved.

 “Computer system” includes “electronic data” that is stored on any of the items described in a. above or temporarily outside of your “computer system” for use by an insured.
- 2. “Confidential corporate information” means any commercial trade secret, data, design, interpretation, forecast, formula, method, practice, process, record, report or other item of information of a third party which is:
 - a. Not available to the general public; and
 - (1) Provided to you under a mutually agreed to written confidentiality or non-disclosure agreement; or
 - (2) Marked confidential or otherwise specifically designated in writing as confidential by such third party.

3. "Electronic Data" means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.
4. "Network Security or Data Breach Event" means:
 - a. Transmission of malware from your "computer system" to a third party;
 - b. The inability of an authorized user to access your website or your "computer system" because of a denial of service attack; or
 - c. A "privacy event".

As used in this definition, a denial of service attack means a malicious attack intended by the perpetrator to overwhelm the capacity of your "computer system" or website by sending an excessive volume of "electronic data" to such "computer system" or website in order to prevent authorized access to it.

5. "Personally identifiable information" means any:
 - a. Individual's name in combination with any one or more of the following:
 - (1) Social security number;
 - (2) Drivers license number or any other state identification number;
 - (3) Medical or healthcare data including protected health information;
 - (4) Any account number, credit card number or debit card number;
 - (5) Any account relationships, account balances or account histories; or
 - (6) Any password, access code or other security code that would permit access to a financial account.
 - b. Non-public personal information as defined in any part of the following statutes or regulations which regulate the use and protection of non-public personal information (as defined in such statutes or regulations):
 - (1) Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the rules and regulations promulgated thereunder, as amended;
 - (2) Gramm-Leach Bliley Act of 1999 (GLBA) and the rules and regulations promulgated thereunder, as amended; or
 - (3) Other state, federal or local privacy laws requiring reasonable security within a "computer system" for non-public personal information, or a privacy policy limiting the sale, disclosure or sharing of non-public personal information or providing individuals with the right to access or collect non-public personal information.
6. "Privacy Event" means:
 - a. Unauthorized disclosure of, loss of, theft of, or unintentional delivery or exposure to others of "personally identifiable information" or "confidential corporate information" which is in the insured's care, custody or control. Such disclosure, loss, theft or unintentional delivery or exposure to others is limited to information obtained or released directly from your "computer system"; or
 - b. Failure by you to disclose or warn of actual or potential disclosure or misappropriation of "personally identifiable information" or "confidential corporate information", but only if this endorsement covers such disclosure or misappropriation and it resulted directly from **a.** above; or
 - c. Violation or the investigation of a violation of any federal, state or local privacy statute addressing disclosure or misappropriation of "personally identifiable information" or "confidential corporate information", but only if this endorsement covers such disclosure or misappropriation and it resulted directly from **a.** above.
7. "Privacy Event Mitigation Expense" means:
 - a. Reasonable and necessary fees and expenses for:
 - (1) An outside vendor to conduct a computer forensic analysis with reasonable allocation of time and resources to investigate your "computer system" to determine the cause and extent of a "privacy event";
 - (2) An approved crisis management or legal firm to review the "privacy event" and advise you on the appropriate response;
 - (3) Travel by directors, executive officers, partners or employees of the insured which is done to mitigate damage from the "privacy event";
 - (4) Printing, advertising, mailing of materials or other costs to provide notice to affected parties of a "privacy event" for the purposes of maintaining good will or compliance with any notification requirements imposed by law; and

- (5)** Services provided to any individual whose primary identification is the subject of a “privacy event”, but only if the primary purpose of such services is mitigating the effect of the “privacy event”:
 - (i)** Reasonable fees and expenses to establish, maintain and provide call center services;
 - (ii)** Credit file monitoring services; or
 - (iii)** Reasonable fees and expenses for any other service specifically approved by us in writing.
- b.** However, “privacy event mitigation expense” shall not include:
 - (1)** Compensation, fees, benefits or overhead of any insured or employee of any insured;
 - (2)** Costs or expenses that would have been incurred in the absence of the “privacy event”;
 - (3)** Costs or expenses associated with upgrading, maintaining, improving, repairing or remediating any “computer system” as a result of a “privacy event”; or
 - (4)** Costs or expenses associated with upgrading, maintaining, improving, repairing or remediating any procedures, services or property as a result of a “privacy event”.