

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
Product Name: Data Compromise Coverage
Project Name/Number: /

Filing at a Glance

Companies: Great American Alliance Insurance Company, Great American Assurance Company, Great American Insurance Company, Great American Insurance Company of New York

Product Name: Data Compromise Coverage SERFF Tr Num: GRTA-125499413 State: Arkansas
TOI: 01.0 Property SERFF Status: Closed State Tr Num: EFT \$50
Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines) Co Tr Num: CP-AR-0802-DATA State Status: Fees verified and received
Filing Type: Form Co Status: Reviewer(s): Betty Montesi, Llyweyia Rawlins, Brittany Yielding
Author: Julie Seaton Disposition Date: 02/28/2008
Date Submitted: 02/20/2008 Disposition Status: Approved
Effective Date Requested (New): Effective Date (New): 05/01/2008
Effective Date Requested (Renewal): 05/01/2008 Effective Date (Renewal):
State Filing Description:

General Information

Project Name: Status of Filing in Domicile:
Project Number: Domicile Status Comments:
Reference Organization: Reference Number:
Reference Title: Advisory Org. Circular:
Filing Status Changed: 02/28/2008 Deemer Date:
State Status Changed: 02/28/2008
Corresponding Filing Tracking Number:
Filing Description:
Please see exp memo.

Company and Contact

Filing Contact Information

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)

Product Name: Data Compromise Coverage
Project Name/Number: /

Julie Seaton, State Filing Technician jseaton@gaic.com
49 East 4th street (513) 763-7914 [Phone]
Cincinnati, OH 45202 (513) 333-6996[FAX]

Filing Company Information

Great American Alliance Insurance Company CoCode: 26832 State of Domicile: Ohio
580 Walnut Street Group Code: 84 Company Type: P&C
Cincinnati, OH 45202 Group Name: State ID Number:
(513) 369-5000 ext. [Phone] FEIN Number: 95-1542353

Great American Assurance Company CoCode: 26344 State of Domicile: Ohio
580 Walnut Street Group Code: 84 Company Type: P&C
Cincinnati, OH 45202 Group Name: State ID Number:
(513) 369-5000 ext. [Phone] FEIN Number: 15-6020948

Great American Insurance Company CoCode: 16691 State of Domicile: Ohio
580 Walnut Street Group Code: 84 Company Type: P&C
Cincinnati, OH 45202 Group Name: State ID Number:
(513) 369-5000 ext. [Phone] FEIN Number: 31-0501234

Great American Insurance Company of New York CoCode: 22136 State of Domicile: New York
580 Walnut Street Group Code: 84 Company Type: P&C
Cincinnati, OH 45202 Group Name: State ID Number:
(513) 369-5000 ext. [Phone] FEIN Number: 13-5539046

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
Product Name: Data Compromise Coverage
Project Name/Number: /

Filing Fees

Fee Required? Yes
Fee Amount: \$50.00
Retaliatory? No
Fee Explanation:
Per Company: No

COMPANY	AMOUNT	DATE PROCESSED	TRANSACTION #
Great American Alliance Insurance Company	\$0.00	02/20/2008	
Great American Assurance Company	\$0.00	02/20/2008	
Great American Insurance Company	\$50.00	02/20/2008	18068851
Great American Insurance Company of New York	\$0.00	02/20/2008	

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
Product Name: Data Compromise Coverage
Project Name/Number: /

Correspondence Summary

Dispositions

Status	Created By	Created On	Date Submitted
Approved	Llyweyia Rawlins	02/28/2008	02/28/2008

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
Product Name: Data Compromise Coverage
Project Name/Number: /

Disposition

Disposition Date: 02/28/2008
Effective Date (New): 05/01/2008
Effective Date (Renewal):
Status: Approved
Comment:

Rate data does NOT apply to filing.

Overall Rate Information for Multiple Company Filings

Overall Percentage Rate Indicated For This Filing	0.000%
Overall Percentage Rate Impact For This Filing	0.000%
Effect of Rate Filing-Written Premium Change For This Program	\$0
Effect of Rate Filing - Number of Policyholders Affected	0

SERFF Tracking Number: GRTA-125499413 State: Arkansas
 First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
 Company Tracking Number: CP-AR-0802-DATA
 TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
 Product Name: Data Compromise Coverage
 Project Name/Number: /

Item Type	Item Name	Item Status	Public Access
Supporting Document	Uniform Transmittal Document-Property & Casualty	Approved	Yes
Supporting Document	Letter and memo	Approved	Yes
Form	Data Compromise Coverage	Approved	Yes

SERFF Tracking Number: GRTA-125499413 State: Arkansas
 First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
 Company Tracking Number: CP-AR-0802-DATA
 TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
 Product Name: Data Compromise Coverage
 Project Name/Number: /

Form Schedule

Review Status	Form Name	Form #	Edition Date	Form Type Action	Action Specific Data	Readability	Attachment
Approved	Data Compromise Coverage	CP 73 54	11/07	Policy/Coverage New Form		0.00	CP7354LH.pdf



THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

**DATA COMPROMISE COVERAGE
LEGAL AND FORENSIC INFORMATION TECHNOLOGY REVIEW, NOTIFICATION
TO AFFECTED INDIVIDUALS AND SERVICES TO AFFECTED INDIVIDUALS**

Coverage under this endorsement is subject to the following:

Data Compromise Limit: \$50,000 Annual Aggregate

Legal and Forensic Information Technology Review Sublimit: \$ 5,000 Annual Aggregate

Data Compromise Deductible: \$ 2,500 Any one "Personal Data Compromise"

The following is added as an Additional Coverage:

Data Compromise - Covered Cause of Loss

Coverage under this Data Compromise Coverage endorsement applies only if all of the following conditions are met:

1. there has been a "personal data compromise"; and
2. such "personal data compromise" is first discovered by you during the policy period for which this Data Compromise Coverage endorsement is applicable; and
3. such "personal data compromise" is reported to us within sixty days of the date it is first discovered by you.

Data Compromise - Coverages Provided

If all three of the conditions listed above in **Data Compromise - Covered Cause of Loss** have been met, then we will provide you the following coverages. Please note that service providers must be approved by us as described in Additional Condition D. - Service Providers.

1. Legal and Forensic Information Technology Review

We will pay your necessary and reasonable costs for the following outside professional services.

a. Legal Services

Professional legal counsel review of the "personal data compromise" and how you should best respond to it.

b. Forensic Information Technology Services

Professional information technologies review if needed to determine, within the constraints of what is possible and reasonable, the nature and extent of the "personal data compromise" and the number and identities of the "affected individuals."

2. Notification to Affected Individuals

We will pay your necessary and reasonable costs to provide notification of the "personal data compromise" to "affected individuals."

3. Services to Affected Individuals

We will pay your necessary and reasonable costs to provide the following services to "affected individuals."

a. Informational Materials

A packet of loss prevention and customer support information.

b. Help Line

A toll-free telephone line for "affected individuals" with questions about the "personal data compromise" or wanting to request additional services as listed in **c.** and **d.**

c. Credit Report and Monitoring

A credit report and an electronic service automatically monitoring for activities affecting an individual's credit records. This service is subject to the "affected individual" enrolling for this service with the designated service provider.

d. Identity Restoration Case Management

As respects any "affected individual" who is or appears to be a victim of "identity theft" that may reasonably have arisen from the "personal data compromise," the services of an identity restoration professional who will assist that "affected individual" through the process of correcting credit and other records and, within the constraints of what is possible and reasonable, restoring control over his or her personal identity.

Limits

The most we will pay under this Data Compromise Coverage is the Data Compromise Limit indicated for this endorsement.

The most we will pay under **Legal and Forensic Information Technology Review** coverage is the Legal and Forensic Information Technology Sublimit indicated for this endorsement. This sublimit is part of, and not in addition to, the Data Compromise Limit.

The Data Compromise Limit and Legal and Forensic Information Technology Review Sublimit are annual aggregate limits. Those amounts are the most we will pay for the total of all covered costs arising out of all "personal data compromise" events which are first discovered by you during the present annual policy period. These limits apply regardless of the number of "personal data compromise" events occurring during that period.

A "personal data compromise" may be first discovered by you in one policy period but cause covered costs in one or more subsequent policy periods. If so, all covered costs arising from such "personal data compromise" will be subject to the Data Compromise Limit and Legal and Forensic Information Technology Sublimit applicable to the policy period when the "personal data compromise" was first discovered by you.

Coverage for Services to Affected Individuals is limited to costs to provide such services for a period of up to one year from the date of the notification to the "affected individuals." Notwithstanding, coverage for Identity Restoration Case Management services initiated within such one year period may continue for a period of up to one year from the date such Identity Restoration Case Management services are initiated.

Deductible

All coverages provided under this Data Compromise Coverage endorsement are jointly subject to the Data Compromise Deductible indicated for this endorsement.

You shall be responsible for such deductible amount as respects each "personal data compromise" covered under this endorsement.

Exclusions

The following additional exclusions apply to this coverage:

We will not pay for costs arising from the following:

1. Your intentional or willful complicity in a "data compromise."
2. Any criminal, fraudulent or dishonest act, error or omission, or any intentional or knowing violation of the law by you.
3. Any "personal data compromise" occurring prior to the first inception of this Data Compromise Coverage endorsement.
4. Any third party liability or defense costs.
5. Except as specifically provided under coverage **1.b.** Forensic Information Technology Review Services, costs to research any defi-

ciency. This includes, but is not limited to, any deficiency in your systems, procedures or physical security that may have contributed to a "personal data compromise."

6. Costs to correct any deficiency. This includes, but is not limited to, any deficiency in your systems, procedures or physical security that may have contributed to a "personal data compromise."
7. Any fines or penalties. This includes, but is not limited to, fees or surcharges from affected financial institutions.
8. Any criminal investigations or proceedings.
9. Any threat, extortion or blackmail. This includes, but is not limited to, ransom payments and private security assistance.
10. Any virus or other malicious code that is or becomes named and recognized by the CERT Coordination Center, McAfee, Secunia, Symantec or other comparable third party monitors of malicious code activity.
11. Your reckless disregard for the security of "personally identifying information" in your care, custody or control.

Additional Conditions

The following Additional Conditions apply to all coverages under this endorsement.

A. Due Diligence

You agree to use due diligence to prevent and mitigate costs covered under this endorsement. This includes, but is not limited to, complying with reasonable and industry-accepted protocols for:

1. providing and maintaining appropriate physical security for your premises, computer systems and hard copy files;
2. providing and maintaining appropriate computer and Internet security;
3. maintaining and updating at appropriate intervals backups of computer data;

4. protecting transactions, such as processing credit card, debit card and check payments; and
5. appropriate disposal of files containing "personally identifying information," including shredding hard copy files and destroying physical media used to store electronic data.

B. Legal Advice

We are not your legal advisor and do not provide legal counsel to you. None of the services we provide under this coverage constitute legal advice to you. Our determination of what is or is not covered under this Data Compromise Coverage endorsement does not represent advice or counsel from us about what you should or should not do.

C. Pre-Notification Consultation

You agree to consult with us prior to the issuance of notification to "affected individuals." We assume no responsibility under this Data Compromise Coverage for any services promised to "affected individuals" without our prior agreement. If possible, this pre-notification consultation will also include the designated service provider(s) as agreed to under Additional Condition D. Service Providers. You must provide the following at our pre-notification consultation with you:

1. The exact list of "affected individuals" to be notified, including contact information.
2. Information about the "personal data compromise" that may appropriately be communicated with "affected individuals."
3. The scope of services that you desire for the "affected individuals." For example, coverage may be structured to provide fewer services in order to make those services available to more "affected individuals" without exceeding the available Data Compromise Limit.

D. Service Providers

1. We will only pay under this Data Compromise Coverage for services that are provided by service providers approved by us. You must obtain our prior approval

for any service provider whose expenses you want covered under this Data Compromise Coverage. We will not unreasonably withhold such approval.

2. Prior to the Pre-Notification Consultation described in Additional Condition C. above, you must come to agreement with us regarding the service provider(s) to be used for the Notification to Affected Individuals and Services to Affected Individuals. We will suggest a service provider. If you prefer to use an alternative service provider, our coverage is subject to the following limitations:
 - a. such alternate service provider must be approved by us; and
 - b. our payment for services provided by any alternative service provider will not exceed the amount that we would have paid using the service provider we had suggested.

E. Services

The following conditions apply as respects any services provided to you or any "affected individual" by us, our designees or any service firm paid for in whole or in part under this Data Compromise Coverage:

1. The effectiveness of such services depends on your cooperation and assistance.
2. All services may not be available or applicable to all individuals. For example, "affected individuals" who are minors or foreign nationals may not have credit records that can be provided or monitored. Service in Canada will be different from service in the United States and Puerto Rico in accordance with local conditions.
3. We do not warrant or guarantee that the services will end or eliminate all problems associated with the covered events.
4. You will have a direct relationship with the professional service firms paid for in whole or in part under this Coverage. Those firms work for you.

Definitions

With respect to the provisions of this endorsement only, the following definitions are added:

1 **"Affected Individual"** means any person who is your current, former or prospective customer, client, member, director or employee and whose "personally identifying information" is lost, stolen, accidentally released or accidentally published by a "personal data compromise" covered under this endorsement. This definition is subject to the following provisions:

- a. "Affected individual" does not include any business or organization. Only an individual person may be an "affected individual."
- b. An "affected individual" must have a direct relationship with your interests as insured under this Policy. The following are examples of individuals who would not meet this requirement:

1) If you aggregate or sell information about individuals as part of your business, the individuals about whom you keep such information do not qualify as "affected individuals." However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of yours.

2) If you store, process, transmit or transport records, the individuals whose "personally identifying information" you are storing, processing, transmitting or transporting for another entity do not qualify as "affected individuals." However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of yours.

3) You may have operations, interests or properties that are not insured under this Policy. Individuals who have a relationship with you through such other operations, interests or properties do not qualify as "affected individuals." However, specific individuals may qualify as "affected individuals" for

another reason, such as being an employee of the operation insured under this Policy.

- c. An "affected individual" may reside anywhere in the world. However, the coverage and services provided under this endorsement are only applicable and available within the Coverage Territory.

- 2. **"Identity Theft"** means the fraudulent use of "personally identifying information." This includes fraudulently using such information to establish credit accounts, secure loans, enter into contracts or commit crimes.

"Identity theft" does not include the fraudulent use of a business name, d/b/a or any other method of identifying a business activity.

- 3. **"Personal Data Compromise"** means the loss, theft, accidental release or accidental publication of "personally identifying information" as respects one or more "affected individuals," if such loss, theft, accidental release or accidental publication has or could reasonably result in the fraudulent use of such information. This definition is subject to the following provisions:

- a. At the time of the loss, theft, accidental release or accidental publication, the "personally identifying information" must be in your direct care, custody or control.
- b. "Personal data compromise" does not include the loss, theft, release or publication of information that is in the care, custody or control of a third party to whom you have directly or indirectly turned over such information for any reason. This includes, but is not limited to, storage, processing, transmission or transportation of such information.

- c. "Personal data compromise" includes disposal or abandonment of "personally identifying information" without appropriate safeguards such as shredding or destruction, subject to the following provisions:

- 1) your failure to use appropriate safeguards must be accidental and not reckless or deliberate; and
- 2) such disposal or abandonment must take place during the time period for which this Data Compromise Coverage endorsement is effective.

- d. "Personal data compromise" includes situations where there is a reasonable cause to suspect that such "personally identifying information" has been lost, stolen, accidentally released or accidentally published, even if there is no firm proof.

- e. All incidents of "personal data compromise" that are discovered at the same time or arise from the same cause will be considered one "personal data compromise."

- 4. **"Personally Identifying Information"** means information that could be used to commit fraud or other illegal activity involving the credit or identity of an "affected individual." This includes, but is not limited to, Social Security numbers or Account numbers correlated with names and addresses.

"Personally identifying information" does not mean or include information that is otherwise available to the public, such as names and addresses with no correlated Social Security numbers or Account numbers.

All other provisions of this Policy apply.

SERFF Tracking Number: GRTA-125499413 State: Arkansas
First Filing Company: Great American Alliance Insurance Company, ... State Tracking Number: EFT \$50
Company Tracking Number: CP-AR-0802-DATA
TOI: 01.0 Property Sub-TOI: 01.0001 Commercial Property (Fire and Allied Lines)
Product Name: Data Compromise Coverage
Project Name/Number: /

Supporting Document Schedules

Satisfied -Name: Uniform Transmittal Document-Property & Casualty **Review Status:** Approved 02/28/2008

Comments:
Attachment:
ar pctd_1.PDF

Satisfied -Name: Letter and memo **Review Status:** Approved 02/28/2008

Comments:
Attachments:
ar letter_1.PDF
DC Filing Memo Great American CPP 2-6-08.pdf

Property & Casualty Transmittal Document

1. Reserved for Insurance Dept. Use Only	2. Insurance Department Use only
	a. Date the filing is received:
	b. Analyst:
	c. Disposition:
	d. Date of disposition of the filing:
	e. Effective date of filing:
	<input type="checkbox"/> New Business
	<input type="checkbox"/> Renewal Business
	f. State Filing #:
	g. SERFF Filing #:
	h. Subject Codes

3. Group Name Great American Insurance Group	Group NAIC # 084
--	----------------------------

4. Company Name(s)	Domicile	NAIC #	FEIN #	State #
Great American Insurance Company	OH	16691	31-0501234	
Great American Assurance Company	OH	26344	15-6020948	
Great American Insurance Company of NY	NY	22136	13-5539046	
Great American Alliance Insurance Compan	OH	26832	95-1542353	

5. Company Tracking Number	CP-AR-0802-DATA
-----------------------------------	-----------------

Contact Info of Filer(s) or Corporate Officer(s) [include toll-free number]

6. Name and address	Title	Telephone #s	FAX #	e-mail
Julie Seaton	Product Analyst	513.763.7914	513.333.6996	jseaton@gaic.com
49 East 4 th Street Cincinnati, OH 45202				

7. Signature of authorized filer	
8. Please print name of authorized filer	Julie Seaton

Filing information (see General Instructions for descriptions of these fields)

9. Type of Insurance (TOI)	Commercial Property
10. Sub-Type of Insurance (Sub-TOI)	1.0001
11. State Specific Product code(s)(if applicable)[See State Specific Requirements]	
12. Company Program Title (Marketing title)	Data Compromise Coverage
13. Filing Type	<input type="checkbox"/> Rate/Loss Cost <input type="checkbox"/> Rules <input type="checkbox"/> Rates/Rules <input checked="" type="checkbox"/> Forms <input type="checkbox"/> Combination Rates/Rules/Forms <input type="checkbox"/> Withdrawal <input type="checkbox"/> Other (give description)
14. Effective Date(s) Requested	New: 5/1/08 Renewal:

Property & Casualty Transmittal Document---

15.	Reference Filing?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
16.	Reference Organization (if applicable)	N/A
17.	Reference Organization # & Title	N/A
18.	Company's Date of Filing	2/19/08
19.	Status of filing in domicile	<input type="checkbox"/> Not Filed <input type="checkbox"/> Pending <input checked="" type="checkbox"/> Authorized <input type="checkbox"/> Disapproved

20.	This filing transmittal is part of Company Tracking #	CP-AR-0802-DATA
-----	---	-----------------

21.	Filing Description [This area can be used in lieu of a cover letter or filing memorandum and is free-form text]	
-----	---	--

This is a new coverage. It does not replace or supersede any other endorsement or coverage.

Data Compromise Coverage provides a suite of coverages and services that enable an insured commercial entity to respond effectively to a breach of personal information for which that entity is responsible.

One of the largest concerns of business managers across the country today is the possibility that a breach of security could compromise personal information in their care, custody or control. In the past, such a breach might be ignored. Increasingly, however, state laws and media scrutiny require the notification of individuals whose information has been compromised.

All companies hold personal information of individuals. Some companies have personal information just for a small number of people, such as their own employees. Other companies in the course of their business have personal information on many people, such as customers, clients and vendors.

In many states today, companies are required by law to notify affected individuals whose personal information may have been breached. Even in states where no such law currently exists, there is a growing trend on the part of companies that become aware of a breach to notify affected individuals as a sound business practice.

As breach notifications have become more common, there is a growing expectation that the notifying company will provide some level of service to those whose personal information was compromised. The most basic service is a toll-free help line that can be called to ask questions and get information. Often, an offer is made to provide free credit monitoring services for a stated period of time. Sometimes an offer is made to provide affected individuals who become identity theft victims with a case management service to help such individuals regain control over their identities.

Today, a small business entity suffering a personal data breach has a limited range of choices. Some companies attempt to deal with the issue using their own resources. Many hire an outside firm to manage the process and provide the expected services. However, established service firms tend to focus on large companies and often charge minimum fees beyond the means of small businesses.

The program we have created in response to this need is called Data Compromise Coverage. This is an innovative, first party insurance coverage that provides coverage to an insured company that suffers a breach of personal data in their care, custody or control. Coverage includes legal and forensic information technology review of the breach, notification to the affected individuals and services to the affected individuals that include a toll-free help line, one year of credit monitoring service and, for those who become identity theft victims, identity restoration case management services.

Coverage is subject to an annual aggregate limit of \$50,000, with the Legal and Forensic Information Technology Review coverage subject to a sub-limit of \$5,000. There is a per-event deductible of \$2,500.

This endorsement is being filed as an additional coverage. The annual net premium for this coverage varies from \$37 to \$224 per policy based on class of business. Specified classes of business will be ineligible for this coverage. Aside from such ineligible classes, there are no further eligibility requirements and there is no application required.

Enclosed find a copy of the policy endorsement and rule page.

22.	Filing Fees (Filer must provide check # and fee amount if applicable) [If a state requires you to show how you calculated your filing fees, place that calculation below]
	Check #: 399006 Amount: \$50

Specialty Operations
49 East Fourth Street
Dixie Terminal North Building
6th Floor
Cincinnati, OH 45202-3803
PO Box 5425
Cincinnati, OH 45201-5425
1-800-605-6713
513.333.6996 fax



February 19, 2008

Honorable Julie Benafield Bowman
Commissioner of Insurance
Arkansas Insurance Department
1200 West Third Street
Little Rock, Arkansas 72201-1904

Re: Great American Insurance Group		
Great American Insurance Company	084-16691	31-0501234
Great American Insurance Company of New York	084-22136	13-5539046
Great American Assurance Company	084-26344	15-6020948
Great American Alliance Insurance Company	084-26832	95-1542353
Commercial Property		
Form Filing		
<u>GAI Filing # CP-AR-0802-DATA</u>		

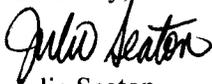
To Whom It May Concern:

The Great American Insurance Group, consisting of the aforementioned companies, hereby places on file the enclosed new form filing for Data Compromise Coverage form. Please see the explanatory memorandum for additional details.

Please find enclosed, for review, the following:

1. Explanatory Memorandum
2. Copies of the Form Pages.
3. All transmittals required by the state.

It is proposed that this filing be applicable to all policies written on or after May 1, 2008. Please return the duplicate of this letter to acknowledge approval and confirm your action. A self-addressed, stamped envelope is enclosed for your convenience.

Sincerely,

Julie Seaton
Product Analyst
513-763-7914
513-333-6996
jseaton@gaic.com

DATA COMPROMISE COVERAGE ENDORSEMENT
FORM NUMBER: CP 7354

This is a new coverage. It does not replace or supersede any other endorsement or coverage.

Data Compromise Coverage provides a suite of coverages and services that enable an insured commercial entity to respond effectively to a breach of personal information for which that entity is responsible.

One of the largest concerns of business managers across the country today is the possibility that a breach of security could compromise personal information in their care, custody or control. In the past, such a breach might be ignored. Increasingly, however, state laws and media scrutiny require the notification of individuals whose information has been compromised.

All companies hold personal information of individuals. Some companies have personal information just for a small number of people, such as their own employees. Other companies in the course of their business have personal information on many people, such as customers, clients and vendors.

In many states today, companies are required by law to notify affected individuals whose personal information may have been breached. Even in states where no such law currently exists, there is a growing trend on the part of companies that become aware of a breach to notify affected individuals as a sound business practice.

As breach notifications have become more common, there is a growing expectation that the notifying company will provide some level of service to those whose personal information was compromised. The most basic service is a toll-free help line that can be called to ask questions and get information. Often, an offer is made to provide free credit monitoring services for a stated period of time. Sometimes an offer is made to provide affected individuals who become identity theft victims with a case management service to help such individuals regain control over their identities.

Today, a small business entity suffering a personal data breach has a limited range of choices. Some companies attempt to deal with the issue using their own resources. Many hire an outside firm to manage the process and provide the expected services. However, established service firms tend to focus on large companies and often charge minimum fees beyond the means of small businesses.

The program we have created in response to this need is called Data Compromise Coverage. This is an innovative, first party insurance coverage that provides coverage to an insured company that suffers a breach of personal data in their care, custody or control. Coverage includes legal and forensic information technology review of the breach, notification to the affected individuals and services to the affected individuals

that include a toll-free help line, one year of credit monitoring service and, for those who become identity theft victims, identity restoration case management services.

Coverage is subject to an annual aggregate limit of \$50,000, with the Legal and Forensic Information Technology Review coverage subject to a sub-limit of \$5,000. There is a per-event deductible of \$2,500.

This endorsement is being filed as an additional coverage. The annual net premium for this coverage varies from \$37 to \$224 per policy based on class of business. Specified classes of business will be ineligible for this coverage. Aside from such ineligible classes, there are no further eligibility requirements and there is no application required.

Enclosed find a copy of the policy endorsement and rule page.