NETGEN
CONSULTING™

WHITE PAPER

July 18, 2016

INSURANCE COMPANY AGENCY AGREEMENT LANGUAGE THAT COULD DRAIN YOUR AGENCY ASSETS

Prepared By:

Judi Newman, Phaze II Consulting, Inc.
And
Bill Larson, Profit Protection Management Consulting

INSURANCE COMPANY AGENCY* AGREEMENT LANGUAGE THAT COULD DRAIN YOUR AGENCY ASSETS

"How much money do you have in your wallet?"

Insurance company agency agreement wording for both Property Casualty agents and Group Health agents require unequivocal compliance with all current state and federal privacy and data breach response laws. Failure to do so puts the agency in potential breach of contract and liable for all claims incurred by the insurance company under the indemnification clause in their agreement. This could cause serious financial harm for most agencies and agency owners.

**Note: Insurance Company agreements between agencies, agents and brokers have many titles. For the purposes of this article, Producer Agreement, Agency Agreement, Agency Contract, Broker Agreement, Independent Agent Agreement and Agent Agreement or any other title will be referenced as "Agency Agreement" (AA). It is important to acknowledge that whatever the agreement is labeled, they all contain similar language on indemnification and hold harmless to the insurance company. Many of these agreements reference the agent party as "Agent", "Producer" or "Broker." For purposes of this article we will refer to these parties as "Agent."*

Agency Agreements may not directly address data beach, but the indemnification clause tends to be one-sided and it typically requires that "the agency hold the company harmless for any claim, demand, liability, dispute, damage, cost, expense or loss including reasonable attorney's fees and cost of litigation arising as a direct result of the acts, errors & omissions and negligence of the Agent."

A periodic review of all insurance company agency agreements should be high on the list of things to do at least annually. Over the past many years, agency agreements have been updated even if no signatures have been required. Addendums to the original agency agreement have been made (most recently through e-mails). Generally, the agency agreements and addendums continue to strengthen the indemnification and hold harmless wording in favor of the company. Sometimes these agency agreements and addendums mention a specific law but most do it in a broader sense to imply compliance to the following:

- Gramm-Leach-Bliley Act (GLB or GLBA)
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Health Insurance Portability and Accountability Act ((HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)

OVERVIEW

Following an extensive review of more than 100 different company agency agreements, most all Property Casualty and Group Health companies require that the agency be compliant with all federal and state laws and more specifically state:

- Property Casualty agency agreements reference the Gramm-Leach-Bliley Act (GLB or GLBA).
- Group Health agency agreements (both individually and agency) cite the Health Insurance and Portability Accountability (HIPAA), Health Insurance Technology for Economic and Clinical Health Act (HITECH). This includes all of the continuing rules being issued for clarification of compliance matters.

MAINTAINING NON PUBLIC PERSONAL INFORMATION

For more than 15 years, ACT has provided information to insurance agents about the need to be in compliance with security issues associated with maintaining nonpublic personal information of clients and employees. In October of 2004 a detailed article was published on the need to be in compliance with GLB Under the laws "compliance is not an option" although many insurance agents have not taken appropriate steps as required by these laws.

http://www.independentagent.com/Resources/AgencyManagement/ACT/Pages/efficient/RealTime/ACTFeb2005.aspx

Even though some agency agreements may cite GLB and HIPAA the compliance wording appears broad enough to include Data Breach Notification laws enacted in 47 states not including Alabama, New Mexico and South Dakota but do include District of Columbia, Guam, Puerto Rico and the US Virgin Islands. These laws have been enacted and are in response to maintaining the privacy of nonpublic personal information, which includes but is not limited to name, date of birth, driver's license numbers and in some cases even a social security number. All insurance agencies are in possession of at least some of this type of information.

In reviewing these privacy laws it is important to point out that failure to comply by the agency would put them in breach of contract and the likely costs to the insurance company would be the responsibility of the agency. The agency would likely face fines and penalties levied by state and/or federal government agencies, depending upon the exact situation. In other words, the numbers could be so significant that it could cause no other alternative than to declare bankruptcy .not only for the business but could impact the agency personally.

AGENCY REQUIREMENTS

PROPERTY CASUALTY AGENCIES

The agency and insurance company relationship begins and ends with the agreement that exists between them. Agency-company agreements are a dynamic area in which contractual provisions change as events and conflicts in the agency-company relationship arise. While agency agreements have come a long way over the last 30 years, there is always room for improvement. Despite any advances, two trends continue to be in play to

this day. The first is the failure of agents to pay much attention to what they are signing when presented an agreement, either a new insurance company for the agency or an updated one from a current arrangement. The second is to how much credence is put into addendums that are attached to the original agreement where a signature is rarely required. Case in point, the addendums sent via email regarding additional security standards for online transactions between the insurance company and the agency.

GROUP HEALTH AGENCY

Prior 2003 agency agreements for agencies involved in the sales and servicing of group health insurance policies had remained the same for at least a decade or more. Upon the passage of HIPAA, and drop dead date for compliance in 2003 most group insurance companies issued addendums to the agreements depicting wording that would advise the agent that they were now a "Business Associate" of the insurance company. In the following few years, group health insurance companies developed and implemented "new" agreements that every agent selling their products needed to sign if they wanted to continue to receive commission because:

- every group health agency involved in the sales and service of group health policies is handling Personal Health Information (PHI); and,
- every group health agency is being held to increasingly higher standards to avoid breaches.

Loss of data for these organizations can lead to regulatory financial repercussions as well as significant reputation damage and insurance companies look to avoid these exposures by passing the liability on to the agency through the agency agreement.

COMPLIANCE FOR ALL INSURANCE AGENCIES

The Gramm-Leach-Bliley Act of 1999 is a robust law and applies to most insurance agents. If an agency is to protect itself from fines, penalties and the possible breach of contract provisions with insurance companies, the agent must comply with the agency agreement and by extension all other relevant laws. Consequently to avoid a breach of the agreement the agency must protect their data described as nonpublic personal information.

> *"The GLBA requires the covered agency, whichever has the relationship to undertake several practices to notify consumers of how their information will be handled and how they will protect that information."*

The following is a partial list of actions that the agency needs to address as part of their compliance effort. **A detailed security plan is at the heart of this effort.**

1. Delivery of privacy statements annually – this explains the agency's privacy practices both internally and with third parties.

2. A written information security plan that is specific and defined.
3. Encryption of all electronic customer information.
4. Encryption of any email that includes nonpublic personal information.
5. Monitoring of systems and procedures to detect actual and attempted attacks into customer information.
6. A data breach response program must be ready to be put into action when it is believed unauthorized individuals have gained access to customer information.
7. Training at least annually of all staff to implement the agency security program.
8. Agencies must have executed agreements with service providers that have access to nonpublic personal information held by the Agency. These agreements verify that the service providers are prepared to protect that information.

Protecting the privacy of consumer information is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999.

BREACH OF CONTRACT

While most agency agreements specifically identify GLB or GLBA others will state "federal and state" privacy and security laws, either way they intend the same thing e.g. "privacy compliance."

In reviewing the agency agreements of over 100 insurance companies, both national and regional in nature, many have gone much further in their agency agreement provisions. The following are examples of specific wording taken directly from a few of the agency agreements reviewed:

> *"The agency will comply with all applicable privacy laws regarding the access of or disclosure of the information provided."*
>
> *"Agency will comply with all applicable federal and state privacy laws to keep confidential all nonpublic personal information. The agency will defend, hold harmless and indemnify the Company against liability, (including without limitation, the Fair Credit Reporting Act and State Privacy Laws and any applicable privacy law) for damages sustained by policyholders and caused by acts or omissions of the Agency."*
>
> *"The agency agrees to indemnify and hold (Insurance Company) harmless from any and all liabilities, losses, damages, fines, penalties expenses and costs including, without limitation, reasonable attorney's fees which they shall suffer, incur, or pay out in connection with any failure by the agency to comply with the terms of the agency agreement."*

Failure to adhere to these provisions puts the agency in a position of "breach of contract" Since none of the agency's own insurance policies like Errors and Omissions or General Liability would provide "breach of contract" coverage, this would be devastating to the agency if a breach of contract was invoked by the insurance company and the agency were found to be at fault.

Typical Indemnification Wording:

As stated earlier, after reviewing in excess of 100 agency agreements, many from group health carriers, the following is typical of every contract we were able to accumulate. We are sure that if we continue to collect this data, it will be almost the same in every instance.

> *"Agency will indemnify and hold harmless company and any affiliate, trustee, officer, director, employee, volunteer or agent from and against any lawsuits, damages, losses, fines, penalties, claims, causes of action, liabilities, costs or expenses, including attorney's fees and court or proceeding costs (collectively, Claims) arising out of or in connection with Agency's negligence, willful acts or omissions."*
>
> *"Any breach of the terms of this agency Agreement or unauthorized or illegal act, violation of Applicable Law, misrepresentation and/or omission by Agency or any or entity under Agency's control (including employees and subagents), including without limitation, any unauthorized use or disclosure of PHI or any failure in security measures affecting PHI"*
>
> *"Agency acknowledges that, effective the later of the Effective Date of this Agency Agreement of February 17, 2010, it shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with any of the safeguards, security, use and disclosure requirements of this Agency Agreement and any guidance issued by the Secretary from time to time with respect to such safeguards, security, use and disclosure requirements."*
>
> *"Agency shall indemnify the Company and hold it harmless from and against any penalties, losses, claims, damages or liabilities (or actions in respect thereof) to which the Company may become subject insofar as such penalties, losses, claims, damages or liabilities (or actions in respect thereof) that arise out of or are based upon any Breach or unauthorized use or disclosure of PHI or Confidential Information by the Agency including its employees, officers, directors, agents, and/or subcontractors."*

These excerpts from various insurance companies clearly are intended to mean that agents are aware that they are liable for the criminal and civil penalties associated with this agreement.

The insurance companies have specifically placed the Hold Harmless and Indemnification wording in their agency agreements to protect themselves by transferring most of the liability exposure to the Agency when the data breach incident appears to be the fault not of the company but of the agency and/or its affiliates, vendors and other business partners.

Compliance with federal and state privacy and data breach laws should not be overlooked. Executing an agency agreement without a complete understanding of all of the compliance requirements of the agreement can be costly to the agency. It is also important to understand that any insurance coverage that the agency might have such as general liability, professional liability or even cyber liability may deny any coverage in these instances.

NOTE: These costs and expenses might likely run hundreds of thousands of dollars, which could cause serious financial damage to most agencies.

COMPLIANCE

PRIVACY PLAN

The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices and to explain how the consumers' non-public information will be protected. In turn, consumers have the right to limit some – but not all – sharing of their information.

The FTC is one of eight federal regulatory agencies that have the authority to enforce the financial privacy law, along with the state insurance authorities. The federal banking agencies, the Securities and Exchange Commission and the Commodity Futures Trading Commission have jurisdiction over banks, thrifts, credit unions, brokerage firms and commodity traders.*

*Keep in mind that company or institution means any organization holding private data even the fact that an individual is a consumer or customer of a particular financial institution is nonpublic person information.

The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most – or all – of the information a company has about them. For example, nonpublic personal information could be information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; insurance applications or information about transactions between the individual and the company.

Whether the privacy statement is on paper or on a website

- It must be reasonably understandable, and designed to call attention to the nature and significance of the information.
- The notice should use plain language, be easy to read, and be distinctive in appearance. A notice on a website should be placed on a page that consumers use

often, or it should be hyperlinked directly from a page where transactions are conducted.

Your notice must accurately describe how you collect, disclose, and protect Non Public Information (NPI) about consumers and customers, including former **customers**. Your notice must include, where it applies to you, the following information:

- Categories of information collected. For example, nonpublic personal information obtained from an application or a third party such as a consumer-reporting agency.
- Categories of information disclosed. For example, information from an application, such as name, address, and phone number; Social Security number; account information; and account balances.
- Categories of affiliates and nonaffiliated third parties to whom you disclose the information. For example, financial services providers, such as mortgage brokers and insurance companies; or non-financial companies, such as magazine publishers, retailers, direct marketers, and nonprofit organizations. You also may describe categories of other nonaffiliated parties to whom you may disclose NPI in the future.
- Categories of information disclosed and to whom under the joint marketing/ service provider exception in section 313.13 of the Privacy Rule (see "**Exceptions**").
- If you are disclosing NPI to nonaffiliated third parties under the exceptions in sections 313.14 (exceptions for processing or administering a financial transaction) and 313.15 (exceptions, including fraud prevention or complying with federal or state law and others) of the Privacy Rule (see "**Exceptions**"), a statement that the disclosures are made "as permitted by law."
- If you are disclosing NPI to nonaffiliated third parties, and that disclosure does not fall within any of the exceptions in sections 313.14 and 313.15, an explanation of consumers and customers' right to opt out of these disclosures (see "**Opt-Out Notices**").
- Any disclosures required by the Fair Credit Reporting Act (see "**Fair Credit Reporting Act**").
- Your policies and practices with respect to protecting the confidentiality and security of NPI (see "**Safeguarding NPI**").

You only need to address those items listed above that apply to you. For example, if you don't share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, you can provide a simplified notice that: (1) describes your collection of NPI; (2) states that you only disclose NPI to nonaffiliated third parties "as permitted by law;" and (3) explains how you protect the confidentiality and security of NPI.

https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

SECURITY PLAN

Every agency is different, and you will need to customize the structure of a security plan to meet the needs of your particular agency.

You will need to identify the threats that the agency likely faces and analyze and prioritize those threats, devise plans and strategies to reduce the likelihood of those threats occurring, have contingency plans ready in case those threats occur.

EXAMPLE SECURITY PLAN TABLE OF CONTENTS

This is the comprehensive table of contents outline for a typical security plan produced by NETGEN Data Security. It is possible depending on the size of the organizations that some agencies may not need all these sections.

I. Executive Summary
Many people will avoid reading a plan until the last minute. The executive summary module allows people to obtain a quick overview of the plan without reading the details.

II. Quick Reference
When something happens, the first question people will ask is *What do I do now?*. This section helps them find the answer quickly.

III. Introduction to Security
When people read your plan, they need to understand what you are trying to do and why. An introductory section helps ensure that the reader is familiar with concepts and terminology in the plan.

IV: Aspects of Security
This section could alternatively be moved into an appendix. It discusses the nature of the threats, which need to be considered and common counter-measures that may be deployed.

V. Security Risk Assessment
This section analyzes the security risks of your organization.

VI. Security Teams
To effectively manage security, it is desirable to assign responsibilities to several members of your agency and as needed organize teams to handle specific aspects of the risk assessment. Some of the teams here can be merged with business continuity teams (if your organization has a business continuity plan) or, if you have a smaller organization, merged with each other.

VII. Actions to Take Now
During the planning and analysis process, a list of actions, which need to be taken will be identified. This is where they go.

VIII. Exercising The Plan
A plan, which only exists on the shelf, or on a hard drive on a server, is not one that will be successfully put into practice when the need arises. This section describes the various methods by which the plan will be tested, exercised, and improved.

IX. Training
The people who will execute the plan need to be trained if the plan is going to successfully be put into action.

X. Maintenance
To ensure that the plan continues to meet the agency's evolving needs and obligations, the plan needs to be periodically reviewed and updated.

XI. Auditing
A plan audit assures everyone that the actions detailed in the plan are being taken, and that the plan meets its requirements. This section discusses and describes how the plan will be audited.

XII. Appendices
There is a lot of information that is useful for the plan reader and for those who will execute the plan, but does not form part of the plan itself. These are some of the appendices that could be included.

1. Security Terms
2. Passwords
3. Policies
4. References
5. Security Checklists

You can never be too prepared when it comes to security. So what are you waiting for?

DATA BREACH RESPONSE PLAN

We have covered a few of the federal laws and regulations with regards to privacy and security on nonpublic personal information (NPI). At a more local level, 47 states and the U. S. Territories of Guam, Puerto Rico and the U. S. Virgin Islands have in place regulations and laws on what a business must do to respond to a known breach. The following link will take you to an overview of the data breach response requirements by state.

https://www.privacyandsecuritymatters.com/wp-content/uploads/sites/6/2016/04/MintzMatrix040116.pdf

All businesses and that includes insurance agencies must have on file in their organization not only a security plan but also a data breach response plan. Although the laws and regulations are state specific, most follow what was put in place in California on July 1, 2003. It is important to remember that along with California most state regulations and laws refer to “unencrypted” NPI. In other words, as long as the data was encrypted it provided the business protection from liability of the data breach. That is changing dramatically. Tennessee in 2016 revised their law to eliminate the encrypted data exception thereby removing the liability protection. Look for most states to follow suit.

Components of the plan can track these elements, although you will want to tailor to the needs of your organization:

- Response team members and Contact Information:
- Procedures for analyzing and containing a potential data security breach:

- Plan for notifying affected individuals:
- Remediation measures to be taken following a data security breach:
- External resources:
  - Legal (e.g. resource to research applicable state laws):
  - Communications
  - IT security/Forensics
- Credit bureau information:
- Insurance information (if any):

So how would your agency respond to such a breach? Do you know the legal requirements for notifying your customers? Should you contact law enforcement? Who do you call first and how long can you wait? Every data breach is different, so there are no specific answers to these questions. A lot will depend on the size of your agency, how many users were impacted, where they live, what kind of data was lost, and so on. However, every agency has the obligation to protect NPI.

The Business Continuity Plan

Natural and manmade disasters underscore the challenges of seamless disaster recovery in the real world. Having a comprehensive business continuity plan isn't just an IT concern; though. Nothing less than the survival of your agency is at stake.

We rarely get a head's up that a disaster is ready to strike. Even with some lead-time, though, multiple things can go wrong; every incident is unique and unfolds in unexpected ways.

This is where a business continuity plan comes into play. To give your organization the best shot at success during a disaster, you need to put a current, tested plan in the hands of all personnel responsible for carrying out any part of that plan. The lack of a plan doesn't just mean your organization will take longer than necessary to recover from an event or incident. You could go out of business for good.

How Business Continuity, Disaster Recovery Plans Differ

Business continuity (BC) refers to maintaining business functions or quickly resuming them in the event of a major disruption, whether caused by a fire, flood, epidemic illness or a malicious attack across the Internet. A BC plan outlines procedures and instructions an organization must follow in the face of such disasters; it covers business processes, assets, human resources, business partners and more.

Many people think a disaster recover plan is the same as a business continuity plan, but a DR plan focuses mainly on restoring IT infrastructure and operations after a crisis. It's actually just one part of a complete business continuity plan, as a BC plan looks at the continuity of the entire organization.

Note that a business impact analysis (BIA) is another part of a BC plan. The BIA essentially helps you look at your entire organization's processes and determine which are most important.

Create a Business Continuity Plan
If your organization doesn't have a BC plan in place, start by assessing your business processes, determining which areas are vulnerable, and the potential losses if those processes go down for a day, a few days or a week. This is essentially a (BIA).

There are six general steps involved in creating a business continuity plan:

1. Identify the scope of the plan.
2. Identify key business areas.
3. Identify critical functions.
4. Identify dependencies between various business areas and functions.
5. Determine acceptable downtime for each critical function.
6. Create a plan to maintain operations.

Remember that the disaster recovery plan is part of the business continuity plan, so check with your IT department to ensure it has or is actively developing a DR plan.

Test Your Business Continuity Plan
You have to rigorously test a plan to know if it's complete and will fulfill its intended purpose. Many organizations test a business continuity plan two to four times a year. The schedule depends on your type of organization, the amount of turnover of key personnel and the number of business processes and IT changes that have occurred since the last round of testing.

Review and Improve Your Business Continuity Plan
Much effort goes into creating and initially testing a BC plan. Once that job is complete, some organizations let the plan sit while other, more critical tasks get attention. When this happens, plans go stale and are of no use when needed.

How to Ensure Business Continuity Plan Support, and Awareness
Every business continuity plan must be supported from the top down. That means senior management must be represented when creating and updating the plan; no one can delegate that responsibility to subordinates.

HIPAA/HITECH BUSINESS ASSOCIATES

DEFINING "BUSINESS ASSOCIATE" FOR INSURANCE AGENTS

Compliance with HIPAA HITECH is not an option for insurance agents who are considered a business associate under the law. Insurance agents involved in the sales and service of group health insurance coverage need only to review any or all of these company agency agreements to see that they are indeed business associates of the insurance companies represented.

With the passage of ARRA (American Recovery and Reinvestment Act of 2009), which included Title VII more commonly referred to as the HITECH Act changed the business associate role to become the same as a covered entity. The reason is HITECH imposes direct legal compliance obligations on business associates. Although this legislation does

not turn business associates into covered entities, it does force—for the first time—direct compliance accountability on business associates, with potential direct civil and criminal penalties for failure to meet these requirements.

Most group health agency agreements now contain the following wording:

"The agency is a business associate and agrees that it is obligated, by law, to meet the applicable provisions of the HIPAA/HITECH law."

The Group Health insurance companies have placed this wording in their agency agreements to protect themselves by transferring much of this liability exposure to the Agency as a "Business Associate." For additional information relative to Group Health Agencies requirements under the HIPAA Omnibus Rule that became effective September 23, 2013 check out the article on ACT

Welcome to ACT - HIPAA Omnibus Rule will have Big Impact on "Business Associates"

SUMMARY OF AGENCY AGREEMENT

As a result of the hold harmless and indemnification sections of most all agency agreements whether property casualty or group health the Agency could be required to pay the following costs and expenses, which would be in addition to the direct cost and expenses incurred by the agency in defense of their action:

- Pay all costs of the investigation by the Company, both of the Agency as well as the costs of a national investigation, since the breach originated at the Agency level
- Pay all costs of the required notifications by the Company
- Pay all costs of attorney fees which, were accrued by the Company
- Pay all defense and liability costs accrued by the Company
- Pay any additional costs accrued by the Company as a result of the Agency's signed agency agreement

If it is found that the agency is required to pay, these payments could cause serious financial harm to most agents.

CONCLUSION

This article is intended to highlight key contractual issues of the insurance agency-company agreements. While we did not provide every detail of the federal and state laws on privacy and security as well as data breach response, it was only our intent to raise the level of awareness of the potential vulnerabilities to the agent in these agreements. To assess the vulnerabilities of your agency a simple survey is available to provide insight into your current compliance status log in to: http://netgensurvey.com

.

Each insurance company will have their own specific legal wording in their agency agreement and, therefore, it is essential that contracts be reviewed before executing them. In this age of data breach, hackers, identity theft and ransom of records, it is time for the insurance agent to take seriously what has only in many instances been given a passing glance.

Technology has provided new and better ways to do business in the agency. What is at stake is the possibility of a data breach, which if it occurs at the agency level could cost the agency enormous amounts of money in fines, penalties as well as the costs incurred by the insurance carrier or carriers. Yes it is possible that a breach at the agency level could affect relationships with more than one insurance company and the costs would be enormous. ACT article

Updated Carrier-Agency Technology Agreements

We hope that the information in this article provides interest in reviewing what your current agreements address. In a recent agency audit, some of the key agreements were dated from the 1980s and 1990s. It is our recommendation that those agreements be updated and we suggest that if you have any that old, it is probably time to dust them off and make sure they fit the times we are operating in today.

Judith "Judi" Newman is president of NetGenDataConsulting. She is also president of Phaze II Consulting, Inc. providing agency management consulting services, merger and acquisition assistance as well as business continuation, perpetuation and sales and marketing planning services. She has worked on site with more than 500 agents across the nation on a variety of consulting projects. Phaze II Consulting Inc. provides consulting services to independent insurance agencies on management issues, operations, planning, valuations and customized projects for individual clients. She can be reached at 239-481-6001 or e-mail judi@netgendatasecurity.com for additional information.

William "Bill" Larson of Profit Protection Risk Management Consulting partnered with Judi to further NetGenDataSecurityConsulting. Bill has 48 years involvement in the insurance industry including 16 years experience consulting in the field of Data Privacy/Security. Bill is president of PPRMC – specializing in protecting corporate/business profits from the effects of the current Data Privacy and Compliance Requirements. Bill has written numerous articles and was national chairperson of the HIPAA Work Group for IIABA/ACT. The HIPAA Work Group defined the Group Health Agencies/Business Associates requirements under the HIPAA Omnibus Rule.

He can be reached at 239-481-6001 or e-mail bill@netgendatasecurity.com for additional information.

***NETGENDATASECURITYCONSULTING** is the result of Judi and Bill realizing that in the world of technology today the small to medium size business has the same data breach exposures, as does a large or multi-national business. No business whether large*

or small is immune to a data breach. While there is a focus on breaches caused from an external source, the biggest percentage of data breaches resulting in potential fines, liability exposures and loss of profits are caused from within the organization. NetGen has developed products and services to assist in the preparation of meeting compliance requirements by insurance agencies for privacy, security and data breach response for most of the state laws as well as federal laws including GLB, FACTA and HIPAA/HITECH. Additional information is available at www.netgendatasecurity.com, we look forward to your visit. Copyright © 2016 NetGen Data Security Consulting

June 20, 2016