March 2020
Volume 2
Issue 1

GIA INSURANCE
SINCE 1892

Galveston Insurance Associates (GIA) Included in IIABA's Best Practices Study

GIA IS PART of an elite group of independent insurance agencies around the United States participating in the Independent Insurance Agents & Brokers of America (IIABA, or the Big "I") "Best Practices" Study Group.

Each year since 1993, IIABA and Reagan Consulting, an Atlanta-based management consulting firm, join forces to study the country's leading agencies in six revenue categories.

The agencies comprising the study groups are selected every third year through a comprehensive nomination and qualifying process and awarded a "Best Practices Agency" designation.

The selected "Best Practices" agencies retain their status during the three-year cycle by submitting extensive financial and operational data for review each year.

"We are proud to be selected as a Best Practices agency," said GIA's president, Garry Kaufman. "Congratulations to all GIA Associates whose hard work and dedication to our clients, community and agency are responsible for this recognition."

More than 1,300 independent agencies throughout the U.S. were nominated to take part in the annual study, but only 267 agencies qualified for the honor.

There are 25 in Texas and GIA is the only agency selected in Galveston County. To be chosen, the agency had to be among the top-performing agencies in one of six revenue categories.

The agency was nominated by either a Big "I" affiliated state association or an insurance company and qualified based on its operational excellence.

The "Best Practices Study" was initiated by the Big "I" in 1993 as the foundation for efforts to improve agency performance.

The annual survey and study of leading independent insurance agencies documents the business practices of the highest-performing agencies and urges others to adopt similar practices.

WELCOME TO OUR NEWSLETTER

We value you and appreciate your business. Our goal is to provide excellent service, competitive pricing, and products tailored to meet the special needs of our clients.

We hope the articles in this edition will provide insight into an array of insurance subjects, and we urge you to contact us with questions and comments.

While we will be focusing on Commercial Lines topics and issues, we will include articles of general insurance interest from time to time.

GIA is a full-service Independent Insurance Agency with dedicated departments for Personal, Commercial and Health coverage.

GIA INSURANCE
SINCE 1892

If you have a coverage question, please call us at:

GIA Insurance
6025 Heards Ln.
Galveston, TX 77551
Phone: (409) 740-1251
Fax: (409) 740-0513

211 W Edgewood Dr, Ste 200
Friendswood TX 77546
Phone: (281) 442-1892
Fax: (409) 740-0513
E-mail: *info@gia-tx.com*

Windstorm Coverage

Important Changes to TWIA Renewal Process

IMPORTANT CHANGES are coming to the Texas Windstorm Insurance Association's (TWIA) renewal process for policies that renew March 1, 2020 and later.

As long as the policyholder's property remains in insurable condition, these changes allow the TWIA to offer renewals directly to policyholders and mortgage companies via US mail, and to accept payment directly from them. The first renewal offers were mailed to TWIA policyholders in January for policies effective March 1.

The policy renewal packet contains the renewal offer, payment coupon, and a cover letter explaining the new process and new TWIA policy contract. The same renewal offer and payment coupon will be mailed to the mortgage company shown on the expiring policy, if applicable. Agents will also receive a copy.

POLICY RENEWAL PROCESS

- **60 days prior to renewal:** Renewal offer mailed to policyholder with a copy to the agent of record and mortgage company.
- **25 days prior to renewal:** Expiration Notice (renewal reminder) mailed.
- **Policy expiration/renewal date:** If coupon and payment are received by TWIA before expiration, the renewal policy goes into effect.
- **10 days after policy expiration:** Policy Lapse Notice mailed.
- If payment is received by TWIA after the original policy expiration, but before the renewal offer expires (30 days), the renewal policy goes into effect with a corresponding lapse in coverage. After 30 days, the policy renewal offer expires and a new application is required.

The renewal offer provides the policyholder and agent the ability to confirm coverage details and make necessary changes as they normally would. Policyholders should contact their agent for questions, changes, premium financing and electronic payments.

How will this affect policyholders?

The policyholder can still work with and submit payment through their agent, but will also now have the ability to mail payment directly to the TWIA.

Changes are also being made to the TWIA policy contract for policies effective on or after 1/1/2020.

One important change is that the TWIA will determine residential replacement cost value at the time a policy is issued, instead of at the time of loss.

For all new and renewal policies issued on or after January 1, 2020, the type of loss settlement, replacement cost value (RCV) or actual cash value (ACV) will be determined at the time a policy is issued.

'The type of loss settlement for policies issued before that date will still be determined at the time a claim is made.

This is great news for policyholders. It will help them know if their property is adequately insured. There can be a big difference between the replacement cost and the actual cash value of a property.

The law requires TWIA policies to be insured at 80% or more of the replacement cost value of the property to qualify for replacement cost coverage.

Determining if insurance to value requirements are met at the time of policy issuance ensures that going into a claim, all parties are aware of whether or not their claim will be settled at replacement cost.

TWIA PAYOUT: *Rebuilding construction in Galveston after Hurricane Ike in 2008.*

Searching Social Media During Hiring Process

IF YOU are hiring, you should not overlook the importance of vetting prospective employees through social networking sites such as Facebook and LinkedIn.

A recent survey by CareerBuilder found that 70% of hiring managers said they had used Facebook or other social networking sites to research job candidates in 2018, up from 60% the year prior. Also, 11% of hiring managers said they planned to start using social networking sites for screening.

With so many people posting their lives online, employers can learn a lot about candidates. There are plenty of legitimate reasons to look at the social networking profiles of prospective hires.

Employees in sales, public relations and customer service serve as representatives for the companies they work for, so employers have a legitimate interest in ensuring potential workers won't embarrass the company,

The most commonly checked social media accounts are Facebook and LinkedIn. Some employers even search for blogs or look at a candidate's Twitter account.

The search can pay off for the employer.

More than half of employers (54%) in the CareerBuilder survey reported finding content on social media that had caused them not to hire a candidate. But also, many employers reported finding positive things on someone's social media accounts that had helped them decide to hire the applicant.

Basic guidelines

Don't overstep – Be warned, though. There is a fine line of overstepping when looking at candidates' social media pages. Here are some tips:

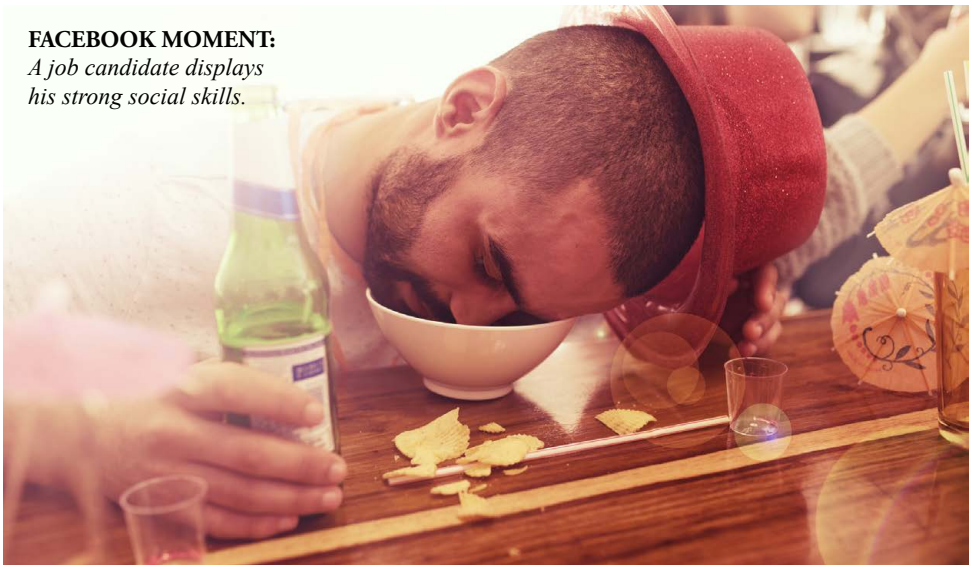
Be fair – Review every applicant in the same manner. If you investigate one applicant's social media accounts, you should look at every applicant's accounts. This is to avoid the appearance of discrimination.

Never ask for access to an applicant's accounts – Demanding passwords could violate a multitude of different laws (a number of states have passed laws barring employers from demanding username and passwords for social media accounts), and could also put the applicant in violation of the terms of service of most of the major social media sites.

In other words, any review should be limited to public information.

Keep it timely - Complete searches later in the hiring process, and preferably after an offer of employment has been made. That sounds counter-productive, but if you learn that an applicant is a protected class by virtue of a social media search, unconscious bias steps in, and you will be in a more difficult position should a discrimination issue arise.

As with any other part of the hiring process, document everything that is done, including saving screen shots of social media pages reviewed.



FACEBOOK MOMENT: *A job candidate displays his strong social skills.*

TOP REASONS FOUND ON SOCIAL NETWORKING SITES FOR CONSIDERING A JOB APPLICANT

- Profile provided a good feel for candidate's personality and fit within the organization: 50%.
- Profile supported the candidate's professional qualifications: 39%.
- Candidate was creative: 38%.
- Candidate showed solid communication skills: 35%.
- Candidate was well-rounded: 33%.
- Other people posted good references about the job candidate: 19%.
- Candidate received awards and accolades: 15%.

TOP REASONS FOUND ON SOCIAL NETWORKING SITES FOR PASSING OVER A JOB APPLICANT

- Candidate posted provocative or inappropriate photographs or information: 53%.
- Candidate posted content about them drinking or using drugs: 44%.
- Candidate bad-mouthed their previous employer, co-workers or clients: 35%.
- Candidate showed poor communication skills: 29%.
- Candidate made discriminatory comments: 26%.
- Candidate lied about qualifications: 24%.
- Candidate shared confidential information from previous employer: 20%.

ONLINE RISKS

Don't Fall Victim to the E-mail Compromise Scam

WEST AFRICAN organized-crime rings have been targeting U.S. business with "business e-mail compromise" scams that are costing firms millions of dollars every year.

Losses to businesses that are targeted by these scams hit an all-time high in the first quarter of 2018, with $685 million in losses reported by 4,081 victims.

That's more than the amount lost for all of 2017 in such scams: $675 million.

The scammers send fake messages to businesses' finance departments claiming to be a vendor for the company with an invoice requiring payment.

These criminals do research before targeting companies, meaning they go to company websites and look for the right people to send e-mails to.

They may even pull annual reports and find what companies they do business with, and then spoof those accounts (meaning they impersonate other firms in the e-mails).

Some criminals will fake a CEO's e-mail account and e-mail that company's finance office ordering payment to a certain account.

In one case cited by *Dow Jones Newswires*, a real estate attorney received an e-mail from the supposed sellers of a local property and asking the lawyer to wire the proceeds of the sale to the criminals' bank account.

The lawyer wired $246,218.83 to the scammers.

The main scams

Money request via compromised CEO account

1. A criminal compromises or spoofs the e-mail account of an executive, such as the CEO.
2. The criminal sends a request for a wire transfer from the compromised account to an employee who is responsible for processing these requests and is subordinate to the executive, such as the controller.
3. The controller submits a wire payment request, as per instructions from his or her "boss."

Invoice from supplier via spoofed e-mail address

A fraudster compromises the e-mail of a business user employed by their target company; for example, someone in accounts payable. This is how it's done:

1. The criminal monitors e-mail of the business user, looking for vendor invoices.
2. The criminal finds a legitimate invoice and modifies the beneficiary information, such as changing the routing number and account number to which payment is to be sent.
3. The scammer then spoofs the vendor's e-mail to submit the modified invoice.
4. Accounts payable, recognizing the vendor name and services provided, processes the invoice and submits a wire request for payment.

HOW TO AVOID GETTING BURNED

- Confirm an e-mailed monetary request purportedly from a company executive by creating a new e-mail and entering their known e-mail address; don't reply to the suspicious e-mail as it will likely go to the criminal.
- The e-mails typically have a similar tone, urging secrecy and expedience. Set up your e-mail gateway to flag key words such as "payment," "urgent," "sensitive" or "secret."
- Look for odd uses of the English language. Many of the scammers are foreigners abroad.
- Although the late-stage e-mails used in these scams may not contain malware, malicious code is often used as part of an overall scheme to initially compromise an employee's e-mail account. So, make sure you have an effective malware detection solution in place.
- Register all domains that are slightly different from the actual company domain.
- Scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.
- Ask accounts payable staff to get to know the habits of your clients, including the details of, reasons behind, and amount of payments.