



Pearl Insurance recently launched a company-wide green initiative to help reduce our ecological footprint. As part of this campaign, and beginning with this second issue of *Risk Control Quarterly*, we have developed a new electronic format for the newsletter, enabling us to reduce paper consumption while still providing you with helpful tips on managing risk for your career and firm.

Pearl and CNA are committed to helping protect our valued customers like you in case of claims and hope you continue to gain valuable knowledge from our extensive collection of risk management tools.

A NEW FORM OF IDENTITY THEFT: RESPONDING TO THE LAWYER IMPERSONATOR

February 2008

By Emily J. Eichenhorn J.D., Senior Risk Control Consultant, CNA
Lawyers Professional Liability, CNA Center, Chicago, IL 60604

Consider the following scenario:

You walk into your office after lunch and settle down at your desk to finish your latte and sort through the day's mail. After opening a few bills and a few payments (oh joy!), you come across an envelope marked "return to sender for insufficient postage." While the envelope appears to be yours, you don't recognize the addressee and do not remember sending anything to that person. When you open the envelope you discover a dummied up version of your letterhead—apparently prepared through cut and paste processes on a computer. The letter is directed at an organization in another town, and says that you, acting as attorney for John Smith, demand that the addressee pay Smith what he is owed under a referenced contract or you will take legal action. The illegible signature is a forgery (you have perfect penmanship), the missive has misspelled words, and the paper is smudged. You never wrote the letter and do not know who John Smith is. You realize that someone (possibly a former client?) with access to a computer and photocopier has apparently created the letterhead either by using some past correspondence from you or cutting and pasting from your website or stealing from your office. While this letter did not reach the addressee, you wonder if Mr. Smith has successfully sent others, to this person or to someone else. Your latte is now cold, and so is the chill up your spine.

What should you do now?

Alarming, this scenario, or a variation thereof, has been reported to CNA by our insureds several times in recent months. The implications are disheartening and disturbing. And your reaction should be swift.

Our advice in the face of these discoveries has been as follows:

- **Start by reporting the situation to the police.** While you may be hesitant because you do not know exactly who may have sent the letter, or even if anything has reached this addressee

or others, you should give the information to the police so that they can investigate. At the least, it appears that someone is attempting to perpetrate a fraud using your name and identity, and having a police report on file may help you resolve any issues that might arise in the future if you are wrongly accused of a crime, or if you need to respond to a disciplinary complaint or file insurance claims.

- **Immediately investigate the potential theft of your personal or business identity.** This may be only one facet of a scheme to use your personal information to acquire any number of other things. At a minimum, talk with the fraud investigators at your credit card company and your bank, and order a credit report to see if there has been any unexpected activity or inquiries into your credit status. Pay close attention to your bills over the next several months to watch for unfamiliar charges. And take note if you seem to stop receiving certain catalogs or other "junk" mail that you've regularly received in the past; it could mean that the catalog company received some sort of change of address request, indicating that the perpetrator opened an account under your name.
- **Contact the attorney registration and disciplinary body in any jurisdiction in which you are licensed.** The idea behind such action is to alert the authorities to the fact that there may be someone improperly using your status as an attorney. It is likely that, if the culprit continues to impersonate you as an attorney and continues to issue communications under your apparent letterhead or forged signature, some recipient of such communication may complain that you have violated some ethics rules. Providing a written statement to the disciplinary authority as soon as you are aware of the situation may help you to quickly resolve or completely avoid any disciplinary proceedings against you arising from such a complaint.

- **Consider contacting the addressee.** But be careful: you want to be mindful of rules against libel or slander. Even if the offending letter references someone you believe to be a former client, or you have some other inkling of who the perpetrator might be, unless you or the police have confirmed it, you don't know who actually sent this letter, and you don't know that anything ever actually reached this addressee. Still, you want the addressee to understand that any letters are not really coming from you, that you do not represent the person referenced in the letter, and that you would appreciate being notified if they receive anything on what appears to be your letterhead, or coming from you in any way. And, if they have received anything else, report that to the police and to the disciplinary board as well.
- **Have your computer system checked for security breaches.** You should consider hiring a forensic computer expert to investigate whether or not your system has been breached. In the incidents CNA has become aware of, the letters were apparently created through simple scanning software and cutting and pasting in a word processor by people the lawyers had had prior contact with. But you want to be alert to the possibility that this incident is only the tip of an iceberg. If someone is able to access your word processing templates through a web portal, for instance, your entire computer system may be at risk.
- **Contact your professional liability insurance carrier,** and – if you carry such coverage – your identity-theft insurance or other IT security breach insurance carrier, to put them on notice of a potential claim. Your identity theft carrier will

likely be able to provide you with further guidance about how to monitor and proceed in the face of further activity.

- **With guidance, draft and issue a cease and desist letter to the perpetrator if you know who it is.** Despite your anger or concern, do not contact the individual directly, even if you have a prior relationship with them. It is best to leave such a contact to the police or one of the fraud investigators you have already contacted. Obtain legal advice regarding the wording of any cease and desist letter to manage the risk of committing libel or slander, and to keep any confrontation as controlled as possible. Be careful not to hinder any police or fraud investigation by stepping in when they would prefer that you not.

So, how can you avoid such a situation in the first place?

It is always difficult to develop strategies to manage against the dishonesty of others. With the scope and sophistication of computer technology readily available to so many, it may be impossible to guard against misappropriation of your business address or identity in this manner. Take measures to guard against computer security breaches to lower the risk that a perpetrator could successfully download your actual letterhead rather than make a poor replica of it. Discuss security with your employees and ask them to be on the lookout for potential problems. Maintain good relationships within the local legal community, especially with opposing counsel, to protect your reputation and offset any damage done by delivery of such a message under your name. And report any potential claims or disciplinary problems to your insurance carriers so that you can take advantage of any loss mitigation your policies may provide.

The purpose of this article is to provide general information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the date of this article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes, or protocols addressed herein unless they are produced or created by CNA.

Any references to non-CNA websites are provided solely for convenience, and CNA disclaims any responsibility with respect to such websites.

To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places, or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions, and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2008 CNA. All rights reserved.



1200 East Glen Avenue
 Peoria Heights, IL 61616
 800.322.2488
 www.pearlinsurance.com