



## **Keep your Eye on the (Other) Ball**

**By Gregory Henshaw, Title Counsel**

I am sure that everyone has been busy preparing your office for the two big issues of the day for the real property practitioner, the implementation and compliance with the ALTA Best Practices and the preparation for the roll out of the TILA/RESPA Integrated Disclosure (TRID). While the preparation for these changes has been time consuming, it has obviously been necessary to maintain the day to day functioning of your office to keep clients and lenders happy. One area in particular that I want to revisit, due to the ever changing threats facing your practice, is the need to be vigilant when it comes to fraud, both from inside and outside of the office. Compliance with the Best Practices, and simple common sense procedures, can help avoid fraudulent activity from within your office or firm. The Best Practices promote specific guidelines for the maintenance of your trust account(s) and the protection of Non-public Personal Information (NPI), and adherence to these guidelines can help to avoid the improper use of NPI and client funds by both authorized and unauthorized personnel.

A much more complicated issue is that of the threat of fraud from sources outside of your office, threats from so-called "fraudsters." Whether hacking, phishing or using good old con man techniques, fraudsters have become increasingly effective at working their way into your office, leaving your trust accounts and client NPI vulnerable to theft. Although we hear reports on a daily basis of the hacking and theft of personal information from large corporations and government entities, it is sometimes easy to be less vigilant when it comes to the safety of your own office. This is especially true when important changes, such as Best Practices and TRID, are front and center and deadlines are looming. Despite the hectic pace of your day, take a few moments to review the procedures you have in place to avoid becoming a victim of the many scams that exist. Be sure to meet with your staff and discuss your safety procedures, as a short meeting today can help avoid a major headache tomorrow. Educate your staff as to the proper way to handle a questionable e-mail, and what to look for in such an e-mail to determine its validity or invalidity. Review your procedures regarding your trust account, as fraudsters are developing ever more creative means of either accessing your accounts or tricking you into allowing them in, or, even worse, wiring funds directly to them.

To help you stay up to date on the latest scams and fraudulent activity affecting your practice, I have attached several fraud alerts from different sources, including from the NC State Bar and First American Title. I have also included a link to the Twitter account for Peter Bolac, Trust Account Counsel at the Bar. (@TrustAccountNC or <https://twitter.com/trustaccountnc> ) A review of these alerts will

give you an idea of what to be aware of, and will demonstrate the lengths that fraudsters will go to in an effort to breach your accounts and other information sources. Just because a specific scam is showing up in another state does not mean that it cannot happen in North Carolina. A fraudster can be operating from anywhere in the world, and, with a single keystroke, cause seemingly endless trouble for the unsuspecting and unprepared practitioner. A real property practice is quickly becoming much more complicated, whether due to new regulations, lender interaction or government oversight. Remember to keep your eye on the other ball, the protection of your trust accounts and client NPI. You can be sure that fraudsters are watching.



*First American Title*

## UNDERWRITING COMMUNICATION

Issued by

*First American Title Insurance Company*

**NC\_2014\_005 - ALERT**

Title: **Email WIRE FRAUD SCAMS**

Issued By: **Palma J. Collins, Senior Southeast Underwriting Counsel**

Date Issued: August 11, 2014

**Purpose:** This notice seeks to alert all First American employees, agents and approved attorneys doing business in the Southeast of another email/internet fraud scheme being perpetrated against title agents and causing loss to title agents, approved attorneys, sellers, lenders and potential buyers/borrowers.

**Advisory:** First American has learned of a scheme in which settlement providers have received emails allegedly from sellers directing the settlement provider to wire the proceeds of sale to institutions not authorized by the seller. We have also learned that lenders have received emails from title agencies purporting to provide wire information for use by the lender to wire loan funds which were not authorized by the settlement provider. The messages were actually emails that were sent by hackers who identified themselves as the seller or settlement provider. The emails appear to be genuine and contain the settlement provider's/seller's email information and/or logos, etc. When the settlement provider and lender transferred their funds pursuant to the fraudulent instructions, their money was stolen with little chance of return. This scam appears to be somewhat similar to the email hacking scheme that came to light earlier this year that targeted real estate agents and those in which hackers infiltrated settlement providers' email to direct purchasers to wire funds to the hackers' accounts.

It is apparent in all of these types of scams that the hackers monitor the email traffic of the agency and/or the customer and are aware of the timing of upcoming transactions. While in the earlier reported instances, customers were induced to misdirect their own funds, now we have reports that settlement providers are being induced to misdirect funds they have an obligation to safe keep.

We strongly recommend that immediate steps are taken to secure computer systems and email accounts and verify with the customer any instruction for disbursement received by email in order to safeguard against this type of scheme. There are a number of government and industry websites that provide tips to protect your systems against cybercrime. Here is a partial list:

[www.onguardonline.gov](http://www.onguardonline.gov)

[www.ic3.gov](http://www.ic3.gov)

**Contact Information for Questions:** If you have any questions concerning this Underwriting Communication, please contact your local underwriting counsel:

**Note to Agents:** While the scope of your agency is limited to the functions of underwriting and the issuance of title insurance policies on our behalf and does not include closing or escrow services, we sometimes provide information and recommendations with regard to your ancillary closing or escrow business as a courtesy to you. Moreover, some communications, depending on whether noncompliance could impact on liability under our policies or closing protection letters, should be considered directives. This communication is being provided to you with those considerations in mind.

**NOTE: This Bulletin is intended for use by title issuing offices, title insurance agents and approved attorneys of First American Title Insurance Company and any reliance by any other person or entity is unauthorized. Should you have any questions regarding this Bulletin, please contact your local First American underwriter.**



*First American  
Title Insurance Company*

## BULLETIN

To: SE/MA Agents and First American employees  
From: SE/MA Underwriting Department  
Date: August 1, 2008  
Bulletin No: FL-562  
Name: Forged Satisfactions; “Naked” Satisfactions, Personally delivered pay-off letters

---

We have received information from MERS that someone has been scanning MERS satisfactions and then taking the MERS officers signatures and cutting and pasting them into satisfactions for mortgages that are not paid. Similar frauds have been reported as to other lenders. We have also had problems with payoff letters delivered by the seller, a realtor or from other “non-traditional sources” which didn’t reflect the full balance.

If a loan has been canceled of record without a corresponding sale or refinance, (a “Naked Satisfaction”) or if you are presented with a mortgage release at or prior to closing (other than directly from the lender); you should:

1. Make specific inquiry of the current owner as to any existing mortgages on the property; and
2. Confirm directly with the mortgage servicer that the mortgage release was validly issued. If the loan is not held by MERS, check with the most recent assignee of record, as shown in the public record.

Human error is a factor, and it is more likely that the replacement mortgage was mis-indexed by the recording office, mis-posted in the search database, or simply missed in the search. As most people are basically honest, a direct question will bring the error to light. You will follow-up by adding the appropriate pay-off requirement(s).

As to checking the validity of a mortgage release:

1. Use independent means to obtain the lender’s telephone number. Do not rely on a phone number supplied by the parties to the transaction. Since you already have a written satisfaction, agents are authorized to rely on verbal confirmations.

2. For mortgages in favor of the Mortgage Electronic Registration Service (MERS) as nominee for a lender, you can verify the release on MERS' website at the following address: <https://www.mers-servicerid.org/sis/> A paid off or foreclosed lien (or otherwise terminated) will show as "inactive" in the search.

If you have ordered a search from First American, our searchers have been instructed when they identify this situation to add a requirement similar to the above as a reminder to our agents.

As to payoff letters received from any "non-traditional" source, thank them politely and obtain your own payoff letter in the normal course.

**NOTE: This Bulletin is intended for use by title issuing offices, title insurance agents and approved attorneys of First American Title Insurance Company and any reliance by any other person or entity is unauthorized. This bulletin is intended solely for the purpose of underwriting policies of First American Title Insurance Company.**



# RED ALERT








## Protect Your Agency from Cyber Fraud

By: Michele Green, VP, Senior Division Underwriting Counsel

The stories regarding hacked email accounts, forged wire instructions, cyber fraud and other risks to your agency continue to be reported at an alarming rate. Protect your agency by keeping these helpful tips near the desk of everyone in your office, especially anyone in charge of wiring money!

In the cyber world, criminals are communicating with you posing as your customers. Worse, they are communicating with your customers posing as YOU.

### DON'T BE A VICTIM! VIGILANCE AND A HEALTHY DOSE OF SKEPTICISM ARE THE BEST WEAPONS IN THE BATTLE AGAINST CYBER FRAUD.

-  **Wire and other disbursement instructions received by email** should be confirmed by telephone at a known or independently-confirmed number, **NOT** the telephone number at the bottom of the email you are trying to confirm.
-  **Consider providing YOUR wire instructions via hard copy only**, with a notation: *With cyber-crimes on the increase, it is important to be ever-vigilant. If you receive an email, or any other communication that appears to be generated from our office, containing new, revised or altered bank wire instructions, consider it suspect and call our office at a number you trust. Our bank wire instructions seldom change.*
-  **Be especially skeptical of any change in wiring instructions.** Who really changes their wire instructions that frequently?
-  **Confirm the account** to which you are wiring is in the name of the party entitled to the funds.
-  **Be suspicious of emails from free, public email account domains** as they are often a source of risk.
-  **Be leery of a new deal coming to your office out of nowhere.**  
*Example: "I have a sales contract and a deposit for property I am purchasing, and I was referred to your office. Will your office act as title and settlement for my transaction?"*  
This conversation is typically followed by a subsequent request to wire out funds originally deposited by check.
-  **Watch out for phishing emails with embedded links**, even when they appear to come from a trusted source such as First American Title.

#### Enter name here

Enter contact information here, click FILE, then SAVE AS.

The information contained in this document was prepared by First American Title Insurance Company ("FATICO") for informational purposes only and does not constitute legal advice. FATICO is not a law firm and this information is not intended to be legal advice. Readers should not act upon this without seeking advice from professional advisers.

First American Title Insurance Company makes no express or implied warranty respecting the information presented and assumes no responsibility for errors or omissions. First American, the eagle logo, First American Title, and firstam.com are registered trademarks or trademarks of First American Financial Corporation and/or its affiliates.

AMD: 04/2015



**First American Title™**

[www.firstam.com](http://www.firstam.com)

©2015 First American Financial Corporation and/or its affiliates. All rights reserved. • NYSE: FAF

**From:** NC State Bar [<mailto:noreply@ncbar.gov>]  
**Sent:** Tuesday, April 21, 2015 3:03 AM  
**To:** Cheryl Jones  
**Subject:** Fraud Alert: Compromised Wiring Instructions



[www.ncbar.gov](http://www.ncbar.gov)

**To: All Members of the North Carolina State Bar**

**From: Peter Bolac, Trust Account Compliance Counsel**

**Last week, the Bar received multiple reports of fraudulent activity relating to wired funds in real estate transactions, with losses as high as \$200,000. Here is a redacted sample of what we have received:**

"On a closing that took place on Friday morning, before we disbursed, we received an email and a phone call from a lady purporting to be our out of state seller asking us to wire funds to her bank account. On Monday we learned that the seller's email was compromised and bad actors had inserted themselves in her place. We attempted to retract the wire and we learned late yesterday that the bank did not retract the wire and will not communicate further without a subpoena."

**This firm had two-level confirmation practices in place to protect against fraudulent wires, but the hackers emailed and called the firm to confirm the wiring instructions as was required. The hackers gained access to the email account of one of the parties to the transaction and learned the necessary information in order to assume the identity of one of the parties and initiate the fraudulent transaction. Another defrauded firm noticed after the fact that the email address of the hacker was different from the actual seller's email address by one letter.**

**One way to protect against this fraud is for the lawyer to initiate the phone call to confirm the emailed wiring instructions, calling only the number in the client file even if a different number is provided via email.**

**Please be vigilant when communicating over email and consider whether your firm's wiring procedures are strong enough to detect and prevent these fraud attempts. If your firm has been the subject of an attempted or successful fraud, please contact me at the State Bar at [pbolac@ncbar.gov](mailto:pbolac@ncbar.gov) or (919) 828-4620.**

**Peter Bolac**

**Trust Account Compliance Counsel**

**North Carolina State Bar**

Please be advised that the contents of this message and any reply may be subject to disclosure under North Carolina law. Informal ethics inquiries and advisories communicated via electronic mail are confidential pursuant to Rule 1.6 of the Rules of Professional Conduct. Attorney Client Assistance Program communications and Lawyer Assistance Program client communications via electronic mail are also treated as confidential pursuant to Rule 1.6 of the Rules of Professional Conduct and N.C. Gen. Stat. 84-32.1.



## New Variation of Fake Check Scam Targets Law Practices

Attorney General Roy Cooper is warning the legal community to be on the lookout for counterfeit check scams after law firms in Gastonia and Oxford recently reported receiving phony checks for \$85,000 and \$295,000 from scammers who asked them to wire the money to bank accounts in Asia.

This latest version of the fraudulent check scam usually begins with an email from someone who claims to be an American living overseas. The sender claims to need legal help with a family problem (such as a dispute over child support), and says that their ex-spouse lives near the attorney's practice. The scammer sends a check and asks the attorney to deposit it, keep a portion of the funds to cover the cost of representing them in court, and send the rest of the money back. The fake checks look very real, even to banks, but ultimately turn out to be counterfeit—meaning that the law firm would be on the hook for any money it sends overseas.

We continue to get reports daily from North Carolina consumers who are the targets of other types of **counterfeit check scams**. Scammers may offer to pay you to cash their checks and send them the money. Or they may "accidentally" overpay for an item you're offering to sell online and then ask you to send back the extra money.

No matter how real a check looks, no matter how legitimate the situation may seem, never cash a check and then send a portion of the money back to the person who sent you the check. If someone asks you to do this, it's a scam. Don't fall for it.

Report fake check scams to the Attorney General's Consumer Protection Division by calling 1-877-5-NO-SCAM or filing a consumer complaint online at [www.ncdoj.gov](http://www.ncdoj.gov).

*This message brought to you on behalf of North Carolina Attorney General Roy Cooper.*

## Trust Accounting

### Bruno's Top Tips: Protect Yourself from Financial Con-Artists

By Bruno DeMolli

*From the 16,3 edition of the Journal*

*"Dear Sir, I am contacting you to seek your assistance and cooperation in the actualization of this rare business opportunity..."*

Many, if not all, of us have received an email over the past few years from someone who appears to be a barely literate Nigerian or Saudi prince begging us for assistance with a financial matter and offering sizeable compensation for doing so. While many immediately recognized this email as a money scam, there are some who jump at the chance of a quick payoff and suffer major financial loss as a consequence. Apparently, when the siren song of a fast buck plays loud enough, it can drown out even the most obvious sounds of warning. In these difficult economic times, lawyers are not immune to falling prey to fraudulent money schemes in the pursuit of an easy and seemingly lucrative payday.

The upsurge of electronic communications over the past decade improved efficiency, saved costs, and allowed for faster information sharing. Unfortunately, the benefits of this new era are tempered by an alarming rise in attempts to defraud law firms. Scam artists have aggressively targeted law firms and lawyers across the country since 2008. Until recently, North Carolina was relatively insulated from this fraudulent activity. However, given the ever-increasing number of reports to the State Bar, it is clear that North Carolina lawyers are now major targets for Internet financial criminals. Lawyers and their trust accounts are consistently targeted by scam artists who pose as potential clients, counterfeit trust account checks, steal account numbers, and forge signatures. Failing to recognize a scam could not only cost a lawyer hundreds of thousands of dollars, it could also result in the use of funds belonging to the lawyer's other clients to cover a counterfeit check—potentially violating the Rules of Professional Conduct.

The most common fraud scheme follows this pattern: Lawyer receives an email from a prospective client from out of the country but with "ties" to the jurisdiction in which the lawyer practices. Most of these schemes propose representation in either a simple debt collection or a divorce settlement. The "client" retains the lawyer to collect a debt from a local company, subtract attorney's fees, and wire the remaining funds back to the "client's" account. Amazingly, before a demand letter is even sent to the bogus debtor, a cashier's check arrives at the lawyer's office paying the debt in full. The lawyer deposits the check in the trust account, receives provisional credit from the firm's bank, subtracts the attorney's fees for a job well done, and, assuming that the cashier's check represents good funds, wires the remaining funds to the "client." By the time the cashier's check is returned by the bank as counterfeit, the "client" has laundered the wired funds through multiple accounts and is long gone.

This scheme has cost lawyers across the country hundreds of thousands of dollars in losses and, in one case, a federal money laundering charge.<sup>1</sup> The State Bar has received reports of this scheme from multiple lawyers and law firms across North Carolina. For example, a firm in Fayetteville was retained on a contingency fee basis by an out-of-state company to collect a debt from a local business. The firm received a bank check for \$300,000 from the debtor and was told to deduct a 10% legal fee and issue a trust account check for the remainder to the client.<sup>2</sup> Smartly, the firm examined the bank check and found it to be fraudulent before depositing the check or making any disbursements, saving the firm's lawyers hundreds of thousands of dollars and a potential serious problem with the State Bar.

Another example: a lawyer in Durham was retained via email by a woman to aid in the collection of a divorce settlement from her ex-husband who allegedly lived out of the country. The lawyer had to do "very little haggling" with the ex-husband before he remitted a certified bank check in the amount of \$297,500, because he did "not want this case to go further involving a lawyer." The lawyer, rightly suspicious, opened a new IOLTA account to protect the lawyer's other clients and deposited the check in the new account. The lawyer attempted to confirm the validity of the check but was only able to verify that the account number, not the actual check, was valid. Thankfully, before the lawyer wired any funds to the "client," the check was returned as counterfeit and the lawyer shut down the IOLTA account without losing the money of his other clients.

Sometimes these schemes occur without the willing participation of the lawyer. The State Bar has received reports of persons printing fraudulent checks on law firm accounts and using them all over the country. For example, a firm in Charlotte was contacted by the fraud department of its depository bank because recently-cashed checks had check numbers that had been previously used. The criminals forged the signature of one of the firm's lawyers on 12 different checks totaling over \$7,000. The firm was reimbursed by the bank for the stolen funds and is working with the bank to prevent similar occurrences in the future.

No lawyer can be 100% protected from criminal activity, but these tips can help safeguard you and your firm against check scams and fraud:

- “Available funds” does not equal collected funds. Even if the bank makes a check’s funds available within two days, it does not guarantee that the actual check will be paid. Fake checks often take up to a week to get returned because scammers put fake routing numbers on the checks.
- Be sure to wire only “collected funds” from your trust account. Wired funds are very hard to recover if a check is returned as counterfeit.
- Closely examine cashier’s checks. Scammers are now counterfeiting certified bank checks from nearly every major and minor bank. For a complete list of counterfeit check alerts, go to the US Treasury Dept. website at [www.occ.treas.gov/news-issuances/alerts/2011/index-2011-alerts.html](http://www.occ.treas.gov/news-issuances/alerts/2011/index-2011-alerts.html).
- Be wary of doing business with out-of-state clients via email. Look for suspicious generic terms in the emails like “your jurisdiction” and for poor grammar.
- Question how the client found you. If the client is requesting services from you which are out of your area of expertise that is a warning sign that something may be awry.
- **MONITOR YOUR TRUST ACCOUNT REGULARLY!** If someone is writing fraudulent checks on your trust account, you should be able to catch it during your monthly review. If you are suspicious of illicit activity, daily or weekly make reviews of your trust account. Keep your staff informed of these scams so they can spot the tell-tale signs of fraud.
- If something seems fishy, it probably is.

By following these tips, knowing your clients, and monitoring your trust account, you can protect your firm and yourself from attacks by Internet financial criminals.

If you believe that your firm has been subject to an attempted or successful fraud, contact the State Bar at (919) 828-4620 and the North Carolina Attorney General’s Office at (919) 716-6000.

#### **Endnotes**

1. Martha Neil, Lawyer Victimized in \$300K Check Fraud is Charged with Money-Laundering, ABA Journal (Aug. 27, 2010).
2. The amount of the check was actually \$298,750. Scam artists will often avoid round numbers in order to make the amount in question appear legitimate.



*First American Title*

## UNDERWRITING COMMUNICATION

Issued by

*First American Title Insurance Company*

### FL-2015-0003 – ADVISORY

Title: **FRAUD ADVISORY – CUSTOMER NPPI**

Issued By: **Florida Underwriting Department**

Date Issued: **February 2, 2015**

#### **Purpose:**

This notice seeks to alert all title policy issuing agents of First American Title Insurance Company relative to recent scams and phishing expeditions asking agents for borrowers' Non-Public Private Information (known as NPPI).

#### **Background:**

Recently, there have been a number of reports of "Fraudsters" seeking personal information on consumers. Through the use of available information (probably through the monitoring of land records), the Fraudster determines that a consumer recently engaged in a loan transaction. The Fraudster then emails or telephones the title agency identified on the documents and, impersonating the borrower, asks for the post-closer handling the file. **Fraudster then requests a copy of the loan application and other information** from the file, stating various reasons which justify the immediate need for such information. The Fraudster then directs the post-closer to email the information/documentation to a specified email address.

If the Fraudster were to successfully receive the requested information, the personal financial information of the borrower could be used to steal identities or commit other crimes.

First American has received multiple incident reports regarding this scam in the past several days. Fortunately, agency employees were able to determine that this was a scam, and prevented any NPPI from leaving the office into the Fraudster's hands.

#### **Advisory:**

It is important that title agencies and their staff safeguard all clients' personal and financial information. NPPI<sup>1</sup> included within settlement files on loan documents and/or other financial data should be kept safe from access by unauthorized parties and not provided to those unaffiliated with the transaction itself. It is recommended that agencies examine their procedures for the protection of NPPI, establish necessary protocols and educate all staff as to these protocols. The attempts described above demonstrate that individual agency employees are being targeted for coercion into releasing this data.

---

<sup>1</sup> Non Public Personal Information (NPPI) is defined in the Gramm-Leach-Bliley Act and generally is any information that is not publicly available. NPPI is more fully defined in the FDIC's Compliance Examination Manual – January 2014, at <https://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf>

**Contact Information for Questions:**

If you have questions or require further information regarding this matter, please contact local underwriting counsel.

---

**NOTE: This Bulletin is intended for use by title issuing offices, title insurance agents and approved attorneys of First American Title Insurance Company and any reliance by any other person or entity is unauthorized**

**\*\*\*This UWC should become a permanent part of your records to assure compliance with its requirements \*\*\***

---