FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

By Lisa A. Tyler
National Escrow Administrator

The Company is experiencing a high volume of emails attempting to have funds wire transferred from operating accounts to pay bills and other expenses. Do not fall victim to the crime! Read "MASQUERADING" to discover what the emails look like.

One of our offices just received an exorbitant phone bill! Yes "TOLL fraud" is on the rise and affecting offices who have not yet upgraded their phone systems to Voice over Internet Protocol (VoIP). The fraudsters hack the voicemail system and sell the numbers to people calling out of the country, or set up auto dialing to numbers that charge by the minute and they get a percentage of the per minute charge.

The bonded promissory notes from 2009 are back again. Actually, the scam involving these notes never left the market, our Company has not encountered them in recent years because they have been tendered by borrowers to their lenders in order to pay their debt in full. Now they are back being tendered in real estate transactions, most recently in Illinois. Read about it in "IT'S baaaack!"

Each month in 2016 this newsletter will include a story describing solutions to the most common issues relating to 1099-S reporting. This month's article "SUBSTITUTE 1099-S form" illustrates the importance of allowing the seller to complete the solicitation form and reporting their real estate sale to the Internal Revenue Service (IRS).

IN THIS ISSUE

Share Fraud Insights
via email, mail or word of mouth.

volume 11 issue 2
February 2016

FRAUD Insights

MASQUERADING

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

Recent cyber related incidents affecting the Company involve email "spoofing" of FNF management, including some senior level executives. The goal of the scheme is to induce an employee to wire funds at the direction of a fraudster impersonating a Company executive.

This is a pretty straight forward Business Email Compromise (BEC) scheme. Notice the display name in the examples reflects an employee name, but the email address is a Gmail™ account. Thankfully, the employees who received the emails noticed the red flags and reported them to the Fraud/Compliance Department.

Attempts have been made to compromise the email accounts of high-level business executives (CFO, CTO, etc.). To date, this has not happened at FNF. The account might be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the Company who is normally responsible for processing these requests.

In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to the bank. This particular version has also been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading" and "Financial Industry Wire Frauds."

The Internet Crime Complaint Center (IC3) suggests the following measures to help both you personally and the Company from becoming victims:

1. Only use Company Web site domain accounts.
2. Be careful what is posted to social media and Company websites, especially job duties/descriptions, hierarchal information and out of office details.
3. Be suspicious of email requests for secrecy or pressure to take action quickly.
   - **a.** Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the email environment to avoid interception by a hacker.
   - **b.** Digital Signatures: Both entities on either side of transactions should use digital signatures. However, this will not work with Web-based email accounts. Additionally, some countries ban or limit the use of encryption.
   - **c.** Delete Spam: Immediately delete unsolicited email (spam) from unknown parties. Do NOT open spam email, click on links in the email or open attachments. These often contain malware that will give subjects access to your computer system.
   - **d.** Forward vs. Reply: Do not use the "Reply" option to respond to any business emails. Instead, use the "Forward" option and either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.
4. Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal email address when all previous official correspondence has been on a Company email, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

EXAMPLE #1

NOT an FNF email address

From: FNF Executive's Name
[mailto:SpoofedFNFUser@gmail.com]
Sent: Wednesday, December 09, 2015 9:55 AM
To: Employee, Real FNF <Real.Employee@fnf.com>; remployee@fnf.com; r.employee@fnf.com
Subject: Wire Payment

Employee,
Are you in the office? I'm in contract meeting and i need you to take care of a wire transfer today..

--
FNF Executive's Name
Senior Executive
Fidelity National Financial, Inc.

NOTICE: The information contained in this message is proprietary and/or confidential and may be privileged. If you are not the intended recipient of this communication, you are hereby notified to: (i) delete the message and all copies; (ii) do not disclose, distribute or use the message in any manner; and (iii) notify the sender immediately.

EXAMPLE #2

NOT an FNF email address

From: FNF Manager's Name
[mailto:srsfence@gmail.com]
Sent: Monday, November 23, 2015 4:32 PM
To: User, Real FNF <UserR@CTT.com>
Subject: Wire Payment

Real User,
Are you in the office? I need you to take care of a wire transfer today..

--
FNF Manager's Name
Important Title
1234 Main Street, Ste. 987
Riverside, CA 92507
Another.User@ltic.com
Phone 0118-999-881-999-119-725-3
Fax (866) 321-4321

Lawyers Title

NOTICE: The information contained in this message is proprietary and/or confidential and may be privileged. If you are not the intended recipient of this communication, you are hereby notified to: (i) delete the message and all copies; (ii) do not disclose, distribute or use the message in any manner; and (iii) notify the sender immediately.

STOP

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

TOLL *fraud*

Last month we shared information regarding "COSTLY area codes" and the "One Ring" scam where the crooks call your cell phone and only allow it to ring once, and then hang up in hopes you will call back. If you call back you are charged international dialing rates.

This month we are providing information on "TOLL fraud" which was originally reported in the June 2014 edition. Toll fraud is rampant and causing hundreds of thousands of dollars in losses to our Company, as a result we are providing more information on the root cause and tips on how to prevent the thieves from running up your office phone bills.

The thieves target companies typically closed on nights and weekends. They call the company and then access each employee's voice mail. They program the employee's direct line to dial a number outside the U.S. – charging the business each time the number is called. Hundreds and even thousands of calls are made. One of our branch offices just experienced this type of fraud and received an exorbitant bill from the telephone company.

In general, toll fraud occurrences can happen in a variety of business sectors, including in FNF's vertical. Even though our users receive training to defend against such tactics, some FNF offices have experienced an occurrence of toll fraud. FNF's Carrier Services Department usually discovers this during their review of the phone bills. In the past few years, the dollar amounts have ranged from small, negligible amounts to larger, more substantial sums; the most recent incident resulted in one of those highly significant amounts.

FNF is fully responsible for all charges relating to toll fraud. While the majority of the telephone services are under a corporate contract, there are some local offices that have signed their own contracts, they have provisions in the contract stating any toll fraud is the sole responsibility of the Company as it stems from their local phone system not being secured.

Typically, the toll fraud happens by the hacker accessing the local voicemail system. Most of these systems were originally setup to allow "pass through dialing," which was put into place for people who were traveling and needed to make Company calls. This allowed a person to dial into the voicemail and receive dial tone to dial another number. Hackers find these holes and sell the telephone numbers hundreds of times using the Internet.

How did the scammers get access? Some offices have older phone equipment and the phones either do not have a passcode set to access voicemail or the passcode set is a generic number. Unfortunately, getting out of paying the fraudulent phone charges is not always easy. Some phone companies will hold customers responsible for all or a portion of the charges and note the customer's equipment was not secure – therefore putting the onus on the victim.

One of our title agents in Indiana recently fell victim to this crime. In one weekend, the fraudsters racked up a litany of long distance charges on the agent's phone bill. Another business (not a title agency) in the same city, had charges over the weekend in excess of half a million dollars.

The scammers made thousands of overseas calls to phone numbers with a set charge to the business each time the number was called – in this particular case the charge was $34.83 per call. The scammers were paid a percentage from each call.

When toll fraud happens the FNF office is informed they are 100% responsible for the charges. Our Company works with the Carrier Services Department to see if any portion of the amount can be written off. Success rate in getting some of the charges written off is 50%, the remaining amounts are negotiated into a payment plan that eases the burden for the local office.

Once we discover that we have fallen victim, we send the following out to the local Information Technology (IT) person and office, and ask that they have their telecom vendor come on-site and perform the following steps:

- Reset all voicemail passwords
  - » Ensure they cannot be changed to 123456 or the same as the extension
- Disable any and all remote access
- Disable all international dialing (except for those that require it) including Canada and Mexico

Our corporate phone system has over 8,000 end users and 400 local offices secured against toll fraud in a few different ways:

- Not allowing the pass through dialing of voicemail or the phone system, only being able to forward your phone to another phone on the system.
- Having calls transferred "mirrored" to a cell phone, which is secured by active directory.
- International dialing is turned off by default and all the known international toll fraud sites are blocked (Dominican Republic, Gabon, Gambia, Congo, Qatar, etc.). If calling one of these locations is required, a Carrier Services Department representative will input the specific number and only that number can be dialed.

FRAUD Insights

IT'S baaaack!

An order is opened at Chicago Title and Trust on December 1, 2015. The buyer in the transaction deposits an international promissory note in the amount of the required deposit of $3.2 million. The escrow closer deposits the item only to have it immediately returned by the bank.

The buyer then provides Processing Instructions that reads as follows:

> *Fiduciary Collector:*
> *This is a prepaid discharge item with an attached charging instrument that has been accepted for value and returned for value, discharge and settlement of account no. 15025574NSJ valued at $3,200,000.0 by the Undersigned, This Exempt Exchange Item [International Promissory Note] is to be presented through electronic medium by FED Wire to access the pre-established Account referenced above. Post the uncollected funds into the asset column of this account and charge the offer and acceptance for settlement; prepaid and exempt when entered in the post-closing balance. Return of original-issue profile is priority-exempt after acknowledgement from the undersigned principal, a Treasury accrual item and a U.S. bankruptcy-proceeding remedy.*

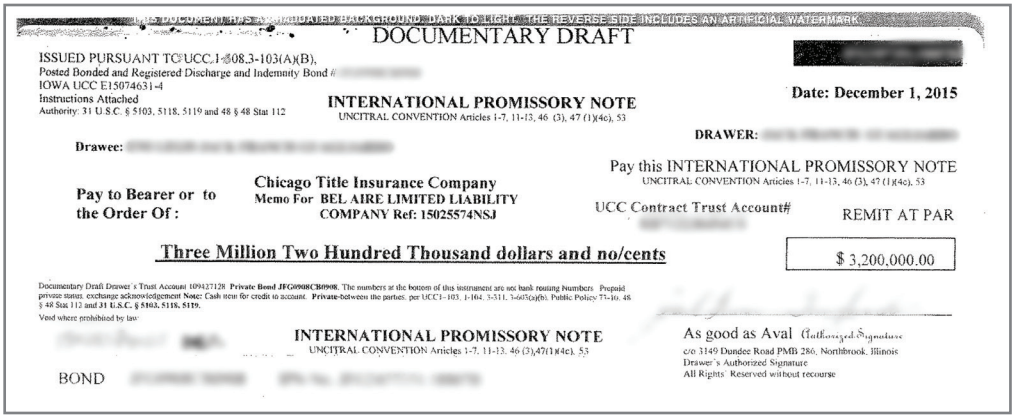
Huh? A quick Internet search reveals a promoter of the international promissory note advertises it as the secret government instrument used to pay your debts using the "government's secret species of money."

The last person who perpetrated this scheme issued more than 2,000 promissory notes for more than $100 million. He was eventually arrested and brought to justice. As reported in the April 2012 edition, he was found guilty of 11 counts of creating false obligations and 10 counts of mail fraud, and faces 30 years in prison.

It is only a matter of time before the latest perpetrator is caught. Regardless, it is clear the buyer and seller in this particular transaction were in cahoots. They attempted to coerce the escrow closer into disbursing the $3.2 million upon receipt of the international promissory note, but their attempt failed when the trust bank refused the deposit.

MORAL OF THE STORY

Settlement agents should remain vigilant and shut down the transaction by resigning as escrow holder immediately if a promissory note is tendered as payment. Settlement agents should not attempt to deposit an international promissory note at the bank. Acting swiftly to cancel the transaction will help sellers put their property back on the market and real estate agents move on to a transaction that will actually close.



DOCUMENTARY DRAFT

ISSUED PURSUANT TO UCC 1-308,3-103(A)(B),
Posted Bonded and Registered Discharge and Indemnity Bond #
IOWA UCC E15074631-4
Instructions Attached
Authority: 31 U.S.C. § 5103, 5118, 5119 and 48 § 48 Stat 112

INTERNATIONAL PROMISSORY NOTE
UNCITRAL CONVENTION Articles 1-7, 11-13, 46 (3), 47 (1)(4c), 53

Date: December 1, 2015

DRAWER:

Drawee:

Pay to Bearer or to the Order Of :

Chicago Title Insurance Company
Memo For BEL AIRE LIMITED LIABILITY COMPANY Ref: 15025574NSJ

Pay this INTERNATIONAL PROMISSORY NOTE
UNCITRAL CONVENTION Articles 1-7, 11-13, 46 (3), 47 (1)(4c), 53

UCC Contract Trust Account#

REMIT AT PAR

Three Million Two Hundred Thousand dollars and no/cents

$ 3,200,000.00

Documentary Draft Drawer s Trust Account 109427128 Private Bond JFG0908CB0908. The numbers at the bottom of this instrument are not bank routing Numbers. Prepaid private status, exchange acknowledgement Note: Cash item for credit to account. Private-between the parties. per UCC1- 103, 1-104, 3-311, 3-603(a)(b). Public Policy 73-10. 48 § 48 Stat 112 and 31 U.S.C. § 5103, 5118, 5119.
Void where prohibited by law

INTERNATIONAL PROMISSORY NOTE
UNCITRAL CONVENTION Articles 1-7, 11-13, 46 (3),47(1)(4c), 53

As good as Aval (Authorized Signature)
c/o 3149 Dundee Road PMB 286, Northbrook, Illinois
Drawer's Authorized Signature
All Rights Reserved without recourse

BOND

SUBSTITUTE 1099-S form

In order to report the sale, the settlement agent must solicit the seller's U.S. Taxpayer Identification Number (U.S. TIN). Our Company solicits this information using the Substitute form 1099-S, an internal form created by the Company. The form was designed in accordance with the regulations to prove compliance and obtain additional information from the seller needed to properly report the sale.

All blanks on the form must be completed by the seller – not the settlement agent – which is why the form does not auto-populate from the production systems. If it is completed by the settlement agent the Company forfeits its opportunity to have penalties abated.

For example, if the seller completes the Substitute 1099-S in their handwriting but accidentally transposes a number in their social security number, the IRS is going to kick back the 1099-S since the U.S. TIN and name does not match. They also impose a penalty of $250. The IRS will waive the fine when they are provided the Substitute 1099-S proving the U.S. TIN used was provided by the seller.

But, if the form is completed in the production system it is obvious the error was made by the settlement agent, not the seller, and the IRS does not waive the penalty. It is crucial settlement agents resist the urge to complete the form on behalf of the seller.