2016 FRAUD, DATA SECURITY AND NPI LEGAL UPDATE
(REV. 09/16)

Fraud Summary:

- Data and payment breaches are increasingly more common and vital business, financial and personal data are being compromised. Malicious fraudsters are using more sophisticated techniques to circumvent various payment systems and target companies and their customers. Even when these criminals are unsuccessful in accessing direct funds, they often have been able to access confidential personal data, allowing them to steal identities of unsuspecting individuals and initiate other elaborate fraud attacks and breach even more secure payment methods.
- Professionals realize how critical it is to keep their organizations' information secure and, as much as possible, prevent breaches of company payment systems. The costs of remediating the impact from payments fraud can be exorbitant and have long-term effects on those companies that fall victim to such malicious attacks.
- A recent national fraud survey produced the following findings:
    - The majority of companies continue to be impacted by payments fraud. 73% of finance professionals report that their organizations were targets of payments fraud in 2015.
    - A vast majority of payments fraud originates from outside an organization.
    - Checks continue to be the payment method most often targeted by those committing fraud attacks as well as the method accounting for the largest dollar amount of loss from such fraud. 71% of organizations that experienced attempted or actual payments fraud in 2015 were victims of check fraud.
    - Finance professionals are most concerned about whether mobile payments are a secure payment method. More than three-quarters of survey respondents believe that consumers are concerned about the secureness of mobile payments and therefore are hesitant to wholly embrace these types of payments.
    - 64% of finance professionals report their organizations were exposed to business email compromise (BEC) in 2015.
- Average Losses:
    - In most cases, the potential loss to a company from an attempted payments fraud attack resulted in a relatively small financial loss. For 39% of organizations, the potential loss from fraud in 2014 is estimated to be less than $25,000; for 31% of organizations the potential loss is between $25,000-249,999. The potential loss is $250,000 or more at 19% of organizations.
- Sources of Attempt/Actual Payments Fraud in 2015
    - Outside individual: 65%
    - Business Email Compromise (BEC) 50%
    - Organized crime ring: 15%
    - Third-party/outsourcer: 12%
    - Account takeover: 11%
    - Internal party: 5%
    - Lost of stolen laptop: 2%
    - Compromised mobile device: 2%

- PricewaterhouseCoopers (PwC) Financial Crimes Unit found that between October 2013 and August 2015, total losses due to account takeover exceeded $1.2 billion!
- Important to note: No cybercrime can be carried out without access to DATA! Protect your DATA!
    - Install a firewall – not very effective against today's hackers

- Install anti-virus software - not very effective against today's hackers

REAL ESTATE TRANSACTIONS FRAUD

Types of Fraud

- Check Fraud
- Wire Fraud
- Forged Deeds
- Forged releases
- Mortgage Slamming
- Email Phishing
- Cyber Fraud

Check Fraud

- Checks continue to be the payment method most often targeted by those committing (or attempting to commit) payments fraud. Seventy-seven percent of organizations that experienced attempted or actual payments fraud in 2014 were victims of check fraud. This is a decrease from the 82 percent that suffered check fraud in 2013 and could be attributed to the decline in check use at many organizations. While their use has, indeed, gradually declined in recent years, checks continue to account for 50 percent of business-to-business (B2B) payments in the U.S.
- There are two primary reasons why checks continue to be the payment method of choice. One, organizations' business partners are hesitant to switch to electronic payments. Secondly, those partners are often unwilling to share their bank information. Despite these challenges, the use of checks is expected to continue to decline with the increasing popularity of more efficient payment methods.

Wire Fraud

- Given the numerous data breaches experienced in 2014, an increase in fraud attempts overall was expected. But the reported increase in wire fraud during 2014 is a little surprising; it may reflect fraudsters "shifting their focus" to organizations' accounts payable departments. Fraudsters are resorting to cyberfraud tactics and are conducting research on and creating profiles of company executives, then attempting to send emails with payment instructions to A/P employees that appear to be from the company's CEO or CFO. In this scenario, email addresses may be hacked, or slightly altered, to deceive the employee into complying and making the payment. Fraudsters may also pose as vendors and request that their payment information be changed because of a new bank relationship, etc.

Identify Theft/Impersonation

- Agent sent PA for a cash sale
- Seller on PA not in title
- Agent asked for record owners contact information from seller listed on PA
- PA seller was very hesitant to give it but finally did
- Agent contacted owner informing her that she would have to come into the office to sign deed
- "Owner" seemed nervous stating that she bought the property for the other guy and that she was not owned any money
- Owner caem in the next day and produced a MI license

- Agent could tell it was fake immediately (not thick enough and not all correct information on it)
- Agent ran it under a black light and seal was missing
- Agent informed lady that ID was missing the seal and they would need another form of ID
- Owner said she would go home and get it but never returned

Identity Theft/Impersonation Tips

- Check for identification (maybe even require 2 forms)
- Know what your state licenses and ID contain
- Use a black light
- Use an independent source to verify seller is really the seller
- Use more than electronic means to communicate with seller

Forged Deeds Tips

- Watch for either a recently recorded quitclaim deed or an unrecorded deed brought into closing
- Check notary website to verify notary
- Require new document executed in your presence

Forged Releases

- Check names on release
- See if there is a transaction that corresponds with the release

Mortgage Slamming

- An instance where an underwriter became aware of an individual obtaining multiple commitments for mortgages on the same property
- They issued a bulletin with the name of the individual
- Direct office actually closed on one of the commitments
- The underwriter found an additional 8 commitments in direct and agents offices

Mortgage Slamming Tips

- Close the gap as much as possible
- Watch for underwriter alerts

Emailing Phishing Tips

- Watch out for phishing emails with embedded links, even when they appear to come from a trusted source
- Be leery of a new deal coming to your office out of nowhere. Then it is typically followed by a subsequent request to wire out funds originally deposited by check
- One party's email is hacked
- Small changes made to email address
- Grammatical/syntax errors

Emailing Phishing Examples

- Correct email address is: "mmctitle.com"
- Fraudulent email uses: "mmcctitle.com"

Case Study:

Closing happened June to and email exchange begins June 11 with a person other than the closer:

- **Fraudster**: Good morning processor, We require our proceed wired to our account, Do you have our company account wiring instructions? Thank you,
- **Agent**: We can wire direct to your personal account, did you supply that information to our closer? Or did she give you a check at the closing yesterday?
- **Fraudster**: Yes, we void and trash the voided check as our bank manager advice us to have our proceed wired to our account, please wire to our BOA account information below
- Bank Name: Bank of America
- Bank Address: 123 Main Steet, Royal Oak, MI
- Account Number: 381039959427
- ABA#: 021200339
- Name: AISHWARYA JEWELRY & GOLD TRADING LLC
- Address: 456 South Street, Royal Oak, MI 48073
- Please email wire confirmation once you have it.
- Thanks for your help.
- **Agent**: We cannot wire to this account we have to wire the funds to your personal account, not your business. Your business did not own the property and can only issue funds to the owner of record.
- Please provide the correct information for your personal account when you can so that when we are able to send the wire we have the information on hand.
- **Fraudster**: Our personal joint bank account is barclays bank UK, please let us know if that should be ok so we can provide the wiring instructions.

Once the email exchange started the processor for the agent told the manager that the seller wanted funds wired instead of a check; manager stopped payment on the check; On June 17, agent receives call from Realtor for seller asking why a stop payment was placed on check. Agent discovers seller never sent emails.

Fraud Prevention Tips:

- 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.
- Be especially skeptical of any change in wiring instructions. Who really changes their wire instructions that frequently?
- Confirm that the account to which you are wiring is the name of the party that is entitled to the funds.
- Be especially skeptical of emails from the free "public" email account domains (we're not going to call them out by name, but you know who they are). In nearly every one of our known fraud email occurrences, at least one person involved in the transaction is using one of those mail accounts, an that was the source of the risk.
- How do you provide YOUR wire instructions to customers? Some of our offices and agents have decided to provide wire instructions via hard copy only with a notation along the lines of "with cyber-crimes on the increase, it is important to be ever-vigilant. It you receive an email or any other communication that appears to be generated from [Office] that contains 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."

Our ID Theft Red Flag Map

- Free and clear property
- Cash only or non-institutional lender
- Often vacant property
- Rush closing for a sub-value price
- Vesting deed notarized out of escrow

Be on the Lookout!

- Watch out for the Bad Guys
- Read the Closing Instructions
- Keep the Processes Tight
- Know what we don't know
- Mechanics Liens
- Listen to your Gut

DATA SECURITY AND NPI

The Importance of Data Security and Privacy

- Brokers and Agents collect personal information from clients in order to assist their clients and must appreciate the legal risk associated with it
- What is personal information?
    - Generally, personal information means any information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- Understand the law:
    - Federal laws
        - Although there are currently no federal laws regarding data privacy that specifically apply to real estate associations or brokerages, some may be subject tot eh Identity Theft Red Flags and Address Discrepancy Rules (Red Flag Rules) contained in the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which require creditors, and those who regularly arrange for credit to be provided, to establish policies and procedures to protect against identity theft.
    - Michigan laws
        - Michigan's Identity Theft Protection Act requires an agency to notify an individual if his personal information has been compromised by a security breach if the breach is likely to result in identity theft. Notice must be given without delay.

Key Principles to a Sound Data Security System

- 5 Principles when evaluating/developing your data security program
    - Take stock
    - Scale down
    - Lock it
    - Pitch it
    - Plan ahead
- Take Stock

- The first step in evaluating or developing your security program is to determine is to *take stock* of your situation
  - what type of information do you collect/maintain
  - who maintains and has access to the collected information
  - how do you collect the information

- Scale Down
  - Once you have *taken stock* of the information you are collecting and maintaining, consider whether collecting and retaining such information is actually necessary
    - General Rules
      - If your association or brokerage does not have a legitimate business need for the personally identifying information, don't collect it.
      - If there is a legitimate business need for the information, keep it only as long as it is necessary.
      - Once the business need is over, properly dispose of it.

- Lock it
  - Once you have *taken stock* and *scaled down*, the next stem in evaluating/developing your data security program is *lock it* and protect the personal information you collect and maintain.
  - There are 4 main categories to consider as you work to protect personal information:
    - Physical security
    - Electronic security
    - Employee training
    - Security practices of contractors and service providers
  - (See the checklist for protecting personal information at the end of this packet for more detailed tips and recommendations)

- Pitch it
  - The final step in evaluating/developing your data security program is to *pitch it* – dispose of personal information you no longer need
  - Proper disposal of personal information is an important step under the Federal Trade Commission (FTC) and Michigan Law
    - What is proper disposal?
      - Generally, personal information is properly disposed of if it cannot be read or reconstructed.
        - Paper records should be shredded
        - Electronic records should be destroyed using a wipe utility program or something similar (simply deleting files using the keyboard or mouse commands generally isn't sufficient)

- Conclusion
  - Considering and implementing these 5 key principles will go a long way in limiting you and your brokerage's exposure to liability for improper handling of personal information