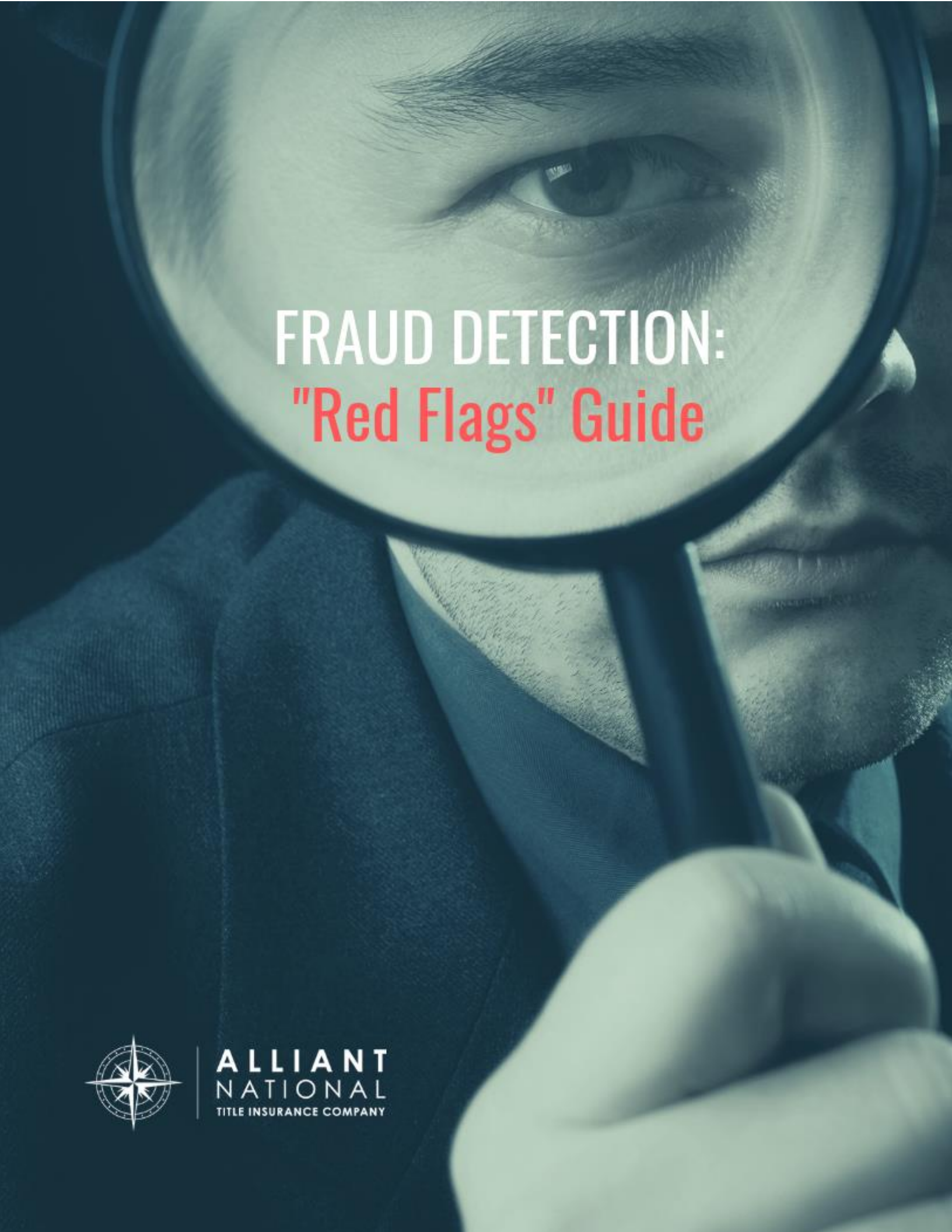

FRAUD DETECTION:
"Red Flags" Guide

ALLIANT
NATIONAL
TITLE INSURANCE COMPANY

FRAUD DETECTION:

"Red Flags"Guide

ALLIANT NATIONAL EDUCATION SERIES

#ALLNATEDU

@alliantnational

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

TABLE OF CONTENTS

INTRODUCTION 1

FRAUD BY PARTIES TO THE TRANSACTION: TRANSACTION FRAUD AND SETTLEMENT FRAUD 2

TRANSACTION FRAUD 2

SETTLEMENT FRAUD 3

GENERAL RED FLAGS 4

SPECIFIC RED FLAGS 5

Detecting and responding to Business Email Compromise / Email Account Compromise 5

What Agents Should Do If Wire Fraud is Suspected After the Exchange of Funds 7

Appraisals 8

Sales Contracts 9

Identity Fraud 10

Preliminary Title Report/Title Search 11

Escrow/Closing Instructions 12

Funds to Close 12

Closing Disclosure/Settlement Statement 13

REFERENCES 14

INTRODUCTION

The independent title agents served by Alliant National have made great strides in fraud prevention, particularly when it comes to preventing wire and escrow frauds. Nevertheless, the threat from fraudsters remains great. According to the FBI, the number of reported victims of email-involved real estate fraud rose more than 1,100 percent from 2015 to 2017. Reported monetary losses rose almost 2,200 percent over the same period.[1]

Our industry remains a prime target for email and other fraudsters, and we know that no one policy or technology solution can ensure the safety of escrow funds in all cases.

This fraud detection guide is meant to assist insurance producers in the critical work of detecting and responding to various types of attempted fraud. This work provides a summary of fraud indicators and "red flags" discussed in other Alliant National publications and Agent Alerts, as well as information from the American Land Title Association (ALTA) and other sources. The general "red flags" listed may emerge at any point during the transaction. Also listed are "red flags" tied to specific types of fraud, or specific stages or documents associated with the transaction.

We hope you find this document helpful as your agency works to implement a comprehensive anti-fraud plan that addresses the realities we face as an industry. We also encourage you to view our growing suite of data security and fraud prevention resources at:
https://alliantnational.com/education/business-email-account-compromise

[1] FBI Internet Crime Complaint Center (IC3) PSA – July 2018

FRAUD BY PARTIES TO THE TRANSACTION: TRANSACTION FRAUD AND SETTLEMENT FRAUD

TRANSACTION FRAUD

Some title fraud may be detected by agents before the transaction closes. Indicators of transaction fraud may include, but are not limited to, the following:

1. Releases of prior mortgages recorded before or independently of the closing of a new loan with no source of payoff funds.
2. Many recent transactions and/or re-recordings.
3. Recent change in title, especially one without concurrent financing.
4. Releases recorded out of sequence.
5. Sale of property subsequent to or concurrent with a divorce.
6. Quitclaim deeds with no consideration.
7. “Intra-family” deeds.
8. Parties to the transaction are affiliated.
9. Document not prepared by an attorney or title company.
10. Document looks non-standard.
11. Power of attorney with Grantee signing as Attorney-in-Fact.
12. Prior signatures indicate failing health or physical deterioration followed by a healthy, strong signature.
13. Bargain purchases—policy amount much higher than purchase price.
14. New mortgage amount much higher than purchase price.
15. Property seller is an LLC/entity/corporation.
16. Appraisal looks questionable (e.g. indicates recent sale/listing activity at significantly lower price; comparable sales are previously flipped properties).

SETTLEMENT FRAUD

Settlement fraud may be detected before closing or at the closing table by the escrow officer. The indicators of this type of fraud may include:

1. Deeds or releases executed before settlement but delivered to the closing without the signer present.
2. Identification other than picture driver's license, or no identification.
3. Recently issued, or suspicious looking Identification cards.
4. Seller not represented by attorney or real estate agent, little closing documentation, no contracts, etc.
5. Seller in a rush.
6. Unusual requests for allocation of proceeds.
7. Land flip—sale shortly after a recent purchase at a much higher price without evidence of significant improvement to the property.
8. Invoices or bills for payment to parties seemingly unconnected to the transaction.
9. Suspicious looking cashier's check presented for closing.

GENERAL RED FLAGS

The presence of any of the following "red flags" may hint that a fraudster is at work in the transaction. The following may emerge at any point:

- Type, spacing, and/or font varies within document from a single source.
- Evidence of "white-out" or other alterations.
- Contains round dollar amounts or "squeezed-in" numbers.
- Any documentation that is difficult to read (e.g., has been copied numerous times and font appears blurry).
- Inconsistencies identified throughout the file (e.g., applicants' names, phone numbers, addresses, Social Security numbers, or handwriting).
- Seller's information doesn't match with the information on file at the property appraiser's office.
- Area code of the seller's phone number is not from the area where they are supposed to reside.
- More than one mortgage lender is reflected throughout the file.
- Parties to the transaction have more than one role (for example, real estate agent is also landlord; employer is also gift donor).
- Applicant appears to be related to another party in the transaction, except the gift donor (for example, verifier of funds or employer, appraiser, escrow officer, etc.).
- Applicants' signatures vary throughout the loan package.
- Unusually long or unusually short loan processing time (brokered loans).
- Patterns or similarities in loan packages received from a specific broker, loan originator, real estate agent or property seller.

SPECIFIC RED FLAGS

Many types of fraud can be recognized by observing their associated specific “red flags.” Types of frauds with associated “red flags” include email-involved fraud, wire fraud, identity fraud and others listed below. Additionally, fraud involving certain elements of the transaction or certain documents are, by their nature, associated with specific kinds of red flags. Among others, the documents and elements of the transaction associated with specific “red flags” include appraisals, the preliminary title report, the closing disclosure and others.

The following is a list of frauds, transaction elements and documents that have specific fraud “red flags.” In some instances, we provide information to help respond when a fraud threat is observed. We encourage you to familiarize yourself with these lists of “red flags” as a means of becoming increasingly vigilant for potential fraud.

DETECTING AND RESPONDING TO BUSINESS EMAIL COMPROMISE / EMAIL ACCOUNT COMPROMISE

Email-involved fraud is a growing issue impacting businesses of all sizes and the general public. The FBI refers to this threat as Business Email Compromise/Email Account Compromise (BEC/EAC). As the name implies, BEC scams are carried out by compromising legitimate business email accounts. The EAC component of the scam refers to the targeting of consumers and the lenders, real estate professionals, attorneys and others who serve them. More information on BEC/EAC fraud prevention and recovery can be found at https://alliantnational.com/education/business-email-account-compromise.

The following is a summary of what agents and their staff members can do to detect and respond to BEC/EAC fraud attempts:

- Exercise extreme caution when weighing any request to change wire instructions. Encourage all parties to do the same (Alliant National Special Alert 15-07).
- Be wary of any email, phone call or other communication that involves threats, high pressure language (e.g. markings, assertions, or language designating the transaction request as
- “Urgent,” “Secret,” or “Confidential,”) or warns of “dire consequences” if immediate action isn’t taken (Alliant National Special Alerts 15-07 and 15-08).
- Be wary of emails with missing or unusual subject lines.
- Be wary of any request to change wiring instructions, especially any last minute requests.

- Be wary of emails that include poor spelling or grammar, are over formal or that are written in a style uncharacteristic of the purported sender. Also, beware of emails that misuse industry terminology, for instance, references to the "HUD" instead of the "Closing Disclosure" (Alliant National Special Alert 15-08).
- Be wary of any unexpected emails or requests, including internal requests purportedly from executives or others (Alliant National Special Alert 15-07).
- Be wary of emails sent at odd hours (Alliant National Special Alert 15-08).
- Be wary of any communication seeking to confirm information the purported sender should already have.
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via a personal email address, it's best to verify the legitimacy of the request via other channels.
- Review monthly escrow statements from your bank (the bank holding the agent's escrow account) as soon as available to verify that all expected funds have actually been received.
- Have a written agreement in place with your bank that the bank will match all names, addresses, account numbers, routing number and the beneficiary bank name on the payment order with where and to whom the funds are actually sent. Or put instructions on the payment order for your bank to verify authorization by matching all of this information.
- Be wary of emailed transaction instructions that direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- Be wary of emailed transaction instructions that direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and of instances where the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- Be wary of emailed transaction instructions delivered in a way that gives the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- Exercise caution when transaction instructions originate from a customer's employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- Exercise caution when a customer's employee or representative emails financial institution transaction instructions on behalf of the customer that are based exclusively on email communications originating from executives, attorneys, or their designees. Additional caution is warranted should the customer's employee or representative indicate he/she has been unable to verify the transactions with such executives, attorneys, or designees.
- Exercise caution when a customer emails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.

Handling of suspicious wire requests (before the exchange of funds)

- Verify all wire instructions with an alternate method of communication.
- Check emails to ensure the sender's address has not been altered. Fraudsters typically use email addresses that closely resemble a seller's (or any party's) actual email address (Alliant National Special Alerts 15-08 and 16-01).
- Do not open unknown or unverified hyperlinks or downloads. Tip: Hovering your mouse over the sender's email address may reveal a different email address (Alliant National Special Alert 15-08). Caution: Do not hover over unknown links within the body of a suspect email. Security experts formerly recommended hovering as a way to determine the validity of such links. However, newer strains of malware may infect a computer when the user merely hovers over the link.
- Delete unsolicited emails from unknown sources.
- In the case of an invoice, verify any changes in vendor payment location and confirm requests for transfer of funds (Alliant National Special Alert 15-07).

WHAT AGENTS SHOULD DO IF WIRE FRAUD IS SUSPECTED AFTER THE EXCHANGE OF FUNDS (REGARDLESS OF THE DOLLAR AMOUNT OF THE LOSS)

- Contact your bank.
    - Speak with someone who has authority to reverse or "recall" the wire. This contact may be in your bank's fraud department. Note: A best practice is to identify this contact and establish a relationship with him or her before a wire fraud incident occurs.
    - Make sure the bank understands you have been the victim of a BEC scheme.
    - Request a Wire Recall or SWIFT Recall Message.
    - Ask your bank to fully cooperate with law enforcement.
- Contact your local FBI office (https://www.fbi.gov/contact-us/field-offices). The FBI has a number of protocols aimed at freezing and retrieving funds. They will activate appropriate protocols based upon the circumstances of the loss. The American Land Title Association has more information on the FBI's protocol for reversing fraudulent international wires.
- Complete and submit a Complaint Referral Form to the FBI's Internet Crime Complaint Center (IC3). Be prepared to provide all details related to the transaction including date, amount, the name of your bank and the beneficiary bank, account numbers, contact information, etc.
- Contact the fraud department at the beneficiary bank to notify them about the wire-recall request due to the fraud. Provide details and request that the account be frozen.
- Contact local law enforcement (https://www.policeone.com/law-enforcement-directory/)
- Contact your Secret Service field office (https://www.secretservice.gov/contact/field-offices/)
- Contact the Alliant National Claims Department by first calling the Claims Manager at (303) 682-9800, ext. 425, and then follow up by emailing applicable information to Claims@alliantnational.com.

When the Money Goes Out, Minutes Count

The 48-hour period following a fraudulent wire transfer is critical; immediately contacting your bank, the local FBI office and submitting a complaint to IC3 as described above will increase your chances of recovering the funds.

Special Handling of International Wires

Since international wire fraud has a very low chance of recovery or reversal of the wire, special precautions are advisable, such as requiring "in-person authorization" from only those authorized signers on an out-going international wire, and having such precautionary requirements agreed upon with your bank.

APPRAISALS

Appraisals and appraisal reports may contain "red flags" indicating potential fraud. "Red flags" may include, but are not limited to:

- Owner of record listed is inconsistent with other information disclosed in the loan file.
- Occupant is identified as a tenant on an owner-occupied refinance application.
- Owner-occupied refinance transaction, but the property is vacant.
- Occupant of subject property is listed as "unknown."
- Appraiser uses public record, exterior inspections, or property seller/builder as sole data sources.
- Illegal zoning is checked on first page of the appraisal.
- "Physical deficiencies or adverse conditions that affect the livability, soundness, or structural integrity box" is checked "Yes" on the first page of the appraisal.
- Subject property has increased in value in a stable or declining market.
- Land value is atypically high for the area.
- Excessive adjustments in urban or suburban area where marketing time is under six months.
- Timeframe between sales does not allow enough time for reported renovations made to property.
- Loan file contains a note with a predetermined value.
- Ineligible Condition (C5, C6) or Quality (Q6) ratings.
- Blank spaces on the form (borrower, client, occupant, etc.).
- Missing photos or maps.
- Photos do not match description of property.
- House number in photo does not match property address.
- Photos do not match the floor plan sketch (i.e. location of garage, fireplace, etc.).
- Photos of subject property taken from odd angles or with no depth of field, or have been cropped or otherwise altered.
- Photos reveal items not disclosed in appraisal (e.g., commercial property next door, railroad tracks, another structure on premises, etc.).

- Weather conditions in photo of property are not appropriate for the date of the appraisal (i.e., July photo shows snow on the ground for a property in Illinois).
- "For rent" or "for sale" sign in photo of subject property on owner-occupant refinance application.
- Most recent sale(s) and/or listing information on subject property and/or comparable properties are missing.
- Use of unverified comparable sales (i.e., not verified through traditional data sources such as MLS, sales office, Closing Disclosure, real estate agent, etc.).
- Use of inappropriate comparable properties (e.g., that are not similar to the subject property when comparable properties are present).
- Excessive distance between comparable properties and subject property.
- All comparable properties are from different town(s) than the subject property.
- Lack of bracketing with comparable sales used (e.g., all sales are significantly larger in living area than the subject).
- Appraisal is ordered and/or prepared prior to date of sales contract or loan application.
- Appraiser is located outside of the county in which the property is located.

SALES CONTRACTS

Sales contract "Red flags" indicating potential fraud may include, but are not limited to:

- Multiple sales contracts exist.
- Sales contract is dated after the appraisal date.
- Sales contract is subject to an existing lease on an owner-occupied transaction.
- Sales contract includes personal property or prohibited sales concessions.
- Sales price is significantly above or below market value.
- Purchase contract addenda adjusts the sales price.
- Applicant is not shown as purchaser.
- No real estate professional involved.
- Real estate agent(s) used, but not paid a fee; or no real estate agent(s) involved at all.
- Seller is a corporation or LLC and the subject property is not new construction.
- Seller is an affiliated real estate agent, trust, relative or employer.
- The parties to the transaction are related by family or commercial enterprise.
- The contract is not dated.
- Names are deleted from or added to the purchase contract.
- The contract is an "option contract."

- The contract was assigned or is assignable.
- Earnest-money deposit is an unusually high amount, consists of the entire down payment, or is an odd amount.
- Contract has a very short inspection period and upon satisfactory inspection, the buyer is to notify the settlement agent who is then supposed to transfer a large portion or all of the deposit to the seller (scam is that 10 business days later, it is discovered that the cashiers' check is counterfeit after the money has been sent, and the escrow account suffers a shortage).
    - Recommendation is to contact the bank or entity issuing the cashier's check to confirm that the cashier's check number and amount is valid prior to depositing the item in the account. Most banks will confirm this by telephone. Due to the increasing occurrences of counterfeit cashier's checks, most banks have instituted mandatory holds on cashier's checks. It is not uncommon for a hold to last up to 10 days (check with your bank to confirm their policy).
- Name and address on earnest-money deposit check is different from that of the buyer.
- Earnest-money deposit checks have inconsistent dates, for example:
    - Check #111 dated November 1
    - Check #113 dated September 1
    - Check #114 dated October 1
- Earnest-money check is not cashed or is not reflected on the Closing Disclosure.

IDENTITY FRAUD

"Red flags" indicating potential identity fraud may include, but are not limited to:

- Borrower lives out of the area and the credit report does not indicate any ties to the area where the property is located.
- Borrower did not attend closing and a Power of Attorney was used.
- Social Security number has not been issued or was issued prior to applicant's date of birth.
- Issue date on Social Security number does not align with the number of years in the workforce.
- Borrower's name is not associated with the Social Security Number.
- Multiple properties are purchased by the same borrower within a short period of time.
- A quit claim deed is used either right before, or soon after, loan closing.
- Vacant land fraud is also a great target for the fraudster because the owners are not at the property and their identity can be easily assumed.
- A request is made post-closing for copies of all the documents, including but not limited to deed, mortgage, note, mortgage application, cancelled checks and other unrecorded documents under some pretext of urgent need. This request could be from a fraudster seeking non-public

information so that he or she can steal someone's information to perpetrate identity theft crimes.
    - A safer potential alternative might be to use a secured password protected portal in which the parties of the transaction are provided with login credentials in order to access their closing documents.
- Suspicion of forgery fraud arises when deeds, mortgage releases or satisfactions are placed of record without any indication of a contemporaneous sale or refinancing of the property within one year of a new transaction (but does not apply to deeds granted from one spouse to another as part of a marital settlement agreement or divorce decree).
    - Recommend requiring a new deed prepared by and executed under the supervision of the settlement agent (put on commitment).
    - Recommend verifying with the mortgage holder that the mortgage release or satisfaction is valid, or that the account has been paid in full and closed.

PRELIMINARY TITLE REPORT/TITLE SEARCH

"Red flags" involving the preliminary title report and title search may include:

- Ordered by, prepared for, or mailed to a party other than the lender.
- Property seller is not in title (possible purchase disguised as a refinance or improper property flip).
- Seller owned property for a short time with a cash-out on the sale.
- Notice of default is recorded (possible cash-out purchase with a straw buyer or foreclosure rescue).
- Report indicates delinquent property taxes.
- Report indicates modification agreement on existing loan(s).
- Title documents show the borrower or Seller on a purchase is not the owner of record.
    - For a purchase transaction, the seller should be the owner of record.
    - For a refinance transaction, the borrower on the loan application should match the owner of record on the title documents.

ESCROW/CLOSING INSTRUCTIONS

"Red flags" involving escrow and closing instructions may include:

- "Fill in the blank" or generic escrow instructions.
- Change of sales prices to "fit" the appraisal.
- Odd amounts paid as a deposit/down payment.
- Significant or unusual buyer credits or fees.
- Unusual amendments to the original transaction.
- Seller on Closing Disclosure different than seller on preliminary title report.
- Evidence of "white-outs" or alterations without initials.
- Payoffs to third parties whose lien was not listed on the preliminary title report.
- Reference to another escrow.
- Down payment is paid into escrow upon opening.
- Cash is paid outside of escrow to property seller.
- Sale is "subject to" property seller acquiring title.
- Entity acting as the property seller is controlled by, affiliated with, or related to the applicant or another party to the transaction.
- Buyer is required to use a specific broker/lender.
- Sale of subject property is not subject to inspection.
- Power of attorney used with no explanation.
- Power of attorney is not properly documented/recorded.

FUNDS TO CLOSE

"Red flags" involving funds to close may include:

- Remitter on cashier's check or source of the wire is not the borrower.
- Cashier's check issued from a bank that is inconsistent with the depository information on application.
- Cashier's check issued from a bank branch that is out of the buyer's geographic area.
- Dollar amount is incorrectly encoded on check.
- Sources of funds are questionable

CLOSING DISCLOSURE/SETTLEMENT STATEMENT

"Red flags" involving the closing disclosure or settlement statement may include:

- Names and addresses of property seller and buyer vary from other loan documentation.
- Seller's mailing address is the same as another party to the transaction.
- Excessive real estate agent commissions paid.
- Real estate commission paid, but no realtors listed on the purchase contract.
- Sales price differs from sales contract.
- Reference is made to undisclosed secondary financing or double escrow.
- Rent prorated on owner-occupied transactions.
- Zero amount due to/from buyer.
- Closing Disclosure or escrow instructions contain unusual credits, disbursements, related parties, delinquent loans paid off, or multiple mortgages paid off.
- Payoffs for items not consistent with liens listed on title commitment.
- Excessive seller paid marketing, administrative, assignment or trust fees.
- Payouts to unknown parties.
- Terms of the closed mortgage differ from the terms approved by the underwriter.
- Date of settlement is delayed without explanation.

REFERENCES

Freddie Mac. (2016, March). Mortgage Screening Process: Red Flags For Single-Family Mortgage Fraud. Retrieved December 21, 2017, from http://www.freddiemac.com/singlefamily/pdf/mortgagescreening_checklist.pdf

Freddie Mac. (2016, July). Fraud Mitigation Best Practices Single-Family. Retrieved December 21, 2017, from http://www.freddiemac.com/singlefamily/pdf/fraudprevention_practices.pdf

TitleNews Online Archive, ALTA (Ed.). (2016, December 15). Colorado Warns of Fraudulent Wire Scams. Retrieved December 21, 2017, from https://www.alta.org/news/news.cfm?20161215-Colorado-Warns-of-Fraudulent-Wire-Scams

Thomas, K. (2017, 1st Quarter). Fraud Against the Real Estate Settlement Service Industry Increases: Protecting Yourself Against Common Frauds. *FLTA Tallahassee Report*, *1*, 3.

American Land Title Association (ALTA) Information Security webpage. (Webpage contains various useful resources to establish and maintain operational readiness; to promote employee awareness and preparation; to provide fraud facts; and to provide useful tools for educating consumers.)