Mortgage Fraud at Financial Institutions: Prevention and Response

By:

Travis P. Nelson[1]

Over the last year law enforcement and regulatory agencies have been inundated with reports of mortgage fraud, occurring in an environment marked by substantial growth in mortgage lending markets and an increase in innovative loan products that have expanded consumer access to home finance. Mortgage loan fraud has become a growing risk for financial institutions, as reported by the Federal Financial Institutions Examination Council ("FFIEC"): "Mortgage loan fraud is growing because it can be very lucrative and relatively easy to perpetrate, particularly in geographic areas experiencing rapid appreciation."[2]

This article will examine the phenomenon of mortgage fraud, basic steps that a financial institution can take toward preventing such fraud, and what remedies a financial institution can pursue in responding to mortgage fraud once detected.

The Nature of Mortgage Fraud

Mortgage loan fraud can generally be divided into two broad categories: fraud for property and fraud for profit. Fraud for property generally involves material misrepresentation or omission of information with the intent to deceive or mislead a lender into extending credit that would likely not be offered if the true facts were known, and is generally committed by home buyers attempting to purchase homes for their personal use.[3] Typical fraud for property schemes include: asset fraud (where a borrower misrepresents their actual assets), occupancy fraud (where a borrower misrepresents that the property is sought as a primary personal residence rather than for investment purposes), employment and income fraud, debt elimination fraud, identity theft, and straw borrowers. Conversely, fraud for profit is motivated by money, committed with the complicity of industry insiders such as mortgage brokers, real estate agents, property appraisers, and settlement agents (attorneys and title examiners).[4] Typical fraud for profit schemes include: appraisal fraud, fraudulent flipping, straw buyers, and identity theft.[5]

---

[1] Travis Nelson (nelsont@pepperlaw.com) is an attorney in the Princeton, NJ office of Pepper Hamilton, LLP, and regularly advises financial institutions on prevention of and responding to mortgage fraud. Mr. Nelson is a former enforcement counsel with the Office of the Comptroller of the Currency.

[2] *The Detection, Investigation, and Deterrence of Mortgage Loan Fraud Involving Third Parties: A White Paper*, Produced by the October 27, 2003 FFIEC Investigations Symposium, Issued February 2005.

[3] *Mortgage Loan Fraud: An Industry Assessment based on Suspicious Activity Report Analysis*, Financial Crimes Enforcement Network ("FinCEN"), November 2006.

[4] *Id*.

[5] Other schemes include: silent second trust, mortgage warehousing, builder bailout, equity skimming, and false down payment.

Though mortgage fraudsters can defeat even the most comprehensive anti-fraud programs, some institutional lapses can also contribute to mortgage fraud, for which regulators have brought enforcement actions, such as for inadequate internal controls, and compliance failures in the areas of customer identification, data security, BSA/AML, and identity theft.

Preventative Measures

In implementing any fraud prevention program, a financial institution should provide all relevant employees with the following:

- Clear directives as to their responsibility when they suspect fraud.
- An awareness of the major types of fraud.
- An understanding of red flags and their use in the application review process.
- A list of resources available to them to detect and investigate fraud.

In structuring the anti-fraud program, the following five points are core global measures that should guide the program:

- **Collecting Data:** Applications must require complete data, which can be used to identify the individual or company during the approval process.
- **Validating Data:** Since personal IDs are sometimes unreliable, and corporate organizing documents can be forged, application data must be validated against credit reports and other trusted third-party sources.
- **Correlating Data:** This process compares various pieces of data with other data on the application, looking for inconsistencies such as an address that does not match the phone number.
- **Detecting Fraud Patterns:** This essential step looks for typical fraud patterns within the application and among third-party information sources. Recently opened credit accounts under the same social security number but different names would be a red flag, suggesting a need for further manual review.
- **Verifying the New Account:** Additional verification to confirm or double-check the individual's intent in opening the account is the final precautionary measure for which various methods can be used.

The FFIEC has issued a comprehensive report for the banking industry on red flags and best practices for combating mortgage fraud.[6] Although the report provides specific examples of red flags and best practices on a scheme-by-scheme basis, the following non-specific red flags are appropriate for most fraud prevention programs:

- The application is unsigned or undated.
- Signatures on credit documents are illegible and no supporting identification exists.
- Borrower has high income with little or no personal property.
- Borrower's age is not consistent with the number of years of employment.
- Borrower has an unreasonable accumulation of assets compared to income or has a large amount of unsubstantiated assets.
- Borrower claims to have no debt.
- Borrower owns an excessive amount of real estate.
- A post office box is the only indicated address for the borrower.
- The same telephone number is used for the borrower's home and business.
- Patterns or similarities are apparent from applications received from other borrowers.
- Borrower does not guarantee the loan or will not sign in an individual capacity.
- Business income is not consistent with business type.
- Years of education is not consistent with borrower's profession.
- Borrower is buying investment properties with no primary residence.

In addition to establishing systems to monitor for red flags, financial institutions should have programs, as applicable, in place that:

- Establish an employee training program that provides instruction on understanding common fraud schemes and recognizing red flags.

---

[6] *The Detection, Investigation, and Deterrence of Mortgage Loan Fraud Involving Third Parties: A White Paper*, FFIEC, Feb. 2005. Though this paper is primarily intended for examiners, its best practices and internal controls guidance are equally appropriate for financial institutions' internal fraud investigation units.

- Conduct pre-funding reviews on new production.
- Closely monitor new borrowers. Scorecard criteria can be used to track performance. Typical tracking data includes: default rates, pre-purchase cycle times, loan quality indicators such as underwriting exceptions, and key data changes prior to approval.
- Closely analyze the borrower's financial information for unusual items or trends.
- Independently verify business information by researching the location and phone number of the business.
- Visit the business location unannounced.
- Employ pre-funding and post-closing reviews to detect any inconsistencies within the transaction.
- Conduct risk based quality control audits prior to funding.
- Ensure that prior liens are immediately paid from new loan proceeds.
- Assess the volume of critical post-closing missing documents.
- Establish a periodic independent audit of loan operations.
- Provide fraud updates/alerts to employees.
- Review patterns on declined loans, i.e., individual social security number, loan officer, etc.
- Establish a fraud hotline for anonymous fraud tips.
- Increase the use of original supporting documentation.

While a determined fraudster will find ways to overcome even the most comprehensive best practices programs, following these points should assist a financial institution that is the victim of mortgage fraud in defending against allegations by regulators that systemic failures led to the fraud.

Mortgage Fraud Through Identity Theft

With the increase in financial institutions' surveillance of account activities, and heightened pressure to "know-your-customer" under customer identification program requirements, mortgage fraudsters are turning to identify theft and identify fraud to perpetrate their schemes. A recent report by FinCEN indicates that 1,761 Suspicious Activity Reports (SAR) were filed between January 1, 2003 and March 31, 2006, with the following distributions:

2003 – 69 reports, 2004 – 466 reports, 2005 – 941 reports, and during the first quarter of 2006 – 855 reports. The data reflects that use of identity theft to perpetrate fraud is on the rise.

Under a typical identity theft mortgage fraud scheme, a fraudster will use the internet to obtain confidential personal information such as social security numbers, addresses and other vital data needed to order a credit report, and then apply for a home equity line of credit on a property owned by the victim and have the loan proceeds wired to an account that can be quickly depleted or transferred to other accounts. All this can be done over the internet, without the victim finding out until the money is long gone. Identity theft is distinguished from identity fraud, which refers to the loan applicant's use of a non-existent social security number or a number taken from the social security death index, along with the use of the borrower's true personal identifiers (name, date of birth, address). The applicant will then use the social security number to qualify for a loan, either because the borrower does not have a number or because the borrower's credit rating associated with their true number is inadequate for approval.

In the late 1990's with the ubiquitous nature of the internet, allowing for the filing of applications for mortgage loans by faceless applicants adrift in cyberspace, and the ease with which fraudsters acquire the tools for identity theft, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (the "Act"), which for the first time specifically labeled identity theft as a crime.[7] Criminal statutes alone were not sufficient to combat the rise of identity theft, so Congress later required federal banking regulators to establish procedures for the identification of possible instances of identity theft.[8] In July 2006, the federal banking agencies offered proposed red flags, which the agencies define as a pattern, practice, or specific activity that indicates the possible risk of identity theft.[9] Whereas some statutory and regulatory sources, both state and federal, decline to provide for a private right of action for victims of identity theft based on an institution's failure to comply with identity theft prevention laws, institutions should consider that the identity theft regulations, as with other privacy and information security regulations and guidance, may establish a new standard of care for potential plaintiffs. Consumers damaged by identity theft where the "red flag" system was not operable, up to date, effective or executed properly are likely to add a count to their complaints that the institution failed to comply with applicable standards of care required by law, forming the basis for measuring an institution's duty of care, a core element in a negligence complaint.

In a recent example of this, on January 17, 2007, retailer TJX Companies, Inc. ("TJX"), announced that its computer network that handles customer transactions for some 2,500 retail stores was hacked into, resulting in the theft of personal credit, debit, and driver's license information. A week later, on January 24, the Massachusetts Bankers Association reported that fraudulent use of the stolen information had been detected overseas. In response, Alabama-

---

[7] 18 U.S.C. § 1028(a).

[8] 15 U.S.C. § 1681m(e)(1)(A)-(B).

[9] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40786 (proposed July 18, 2006).

based AmeriFirst Bank, a TJX customer, filed a lawsuit against TJX,[10] alleging, among other things: (1) common law claims of negligence, breach of contract, and negligence per se, and (2) failure to adhere to the financial institutions customer records privacy and data security safeguards rule of the Gramm-Leach-Bliley Act ("GLBA"). This complaint presents an inventive approach to data processor liability in its use of the federal data security standards as a benchmark against which to assert a negligence per se claim. Under traditional negligence per se analysis under tort law, a plaintiff must show that the defendant's conduct constituted a violation of some statute or regulation, and that the harm resulting from such conduct was the type of harm that the statute or regulation was designed to prevent. Although GLBA and its implementing regulations do not provide for a private right of action, and many state data security statutes do not provide for a private right of action based on failure to comply with such established standards, the data security safeguards contained in the regulations certainly present a measurable and widely accepted standard with which many prominent national users of customer information must comply. As this case demonstrates, the regulators' guidance is having the unintended effect of serving as the basis for supporting common law tort claims against third party providers.[11]

What to Do When Fraud is Discovered

When an institution first discovers fraud, internal corporate security/fraud prevention personnel should collect and copy all relevant documents that pertain to the transaction. This information should include the supporting documents, any parties involved and their suspected roles, and any instruments used in the disbursement of funds. Care should be exercised in preserving the integrity of the documents for their subsequent use by examiners in reviewing the conduct and the institution's response, as well as for use in later administrative or judicial proceedings.

In addition to documentation of the fraud, financial institutions should conduct timely interviews of insiders that may have knowledge of the fraud. As the fraud may be on-going or part of a larger fraud scheme, institutions should consult with counsel, a fraud expert, or their regulator in determining the appropriate strategy for conducting interviews. Interviews of people and entities outside of the institution, if necessary, will be conducted by regulatory and law enforcement authorities, nevertheless institutions can aid in this process by maintaining detailed investigation records to assist regulators.

As soon as a financial institution has a reasonable belief that fraud has occurred, it is required to file a SAR in accordance with the SAR regulation and form.[12] The obligation to file

---

[10] *AmeriFirst Bank v. TJX Companies, Inc.*, Case 1:07-cv-10169-JLT, filed 01/29/2007 (D. Mass)

[11] *See also*, *Patrick v. Union State Bank*, 681 So.2d 1364 (Ala. 1995), *Huggins v. Citibank*, 585 S.E.2d 275 (S.C. 2003), and *Eisenberg v. Wachovia Bank, N.A.*, 301 F.3d 220 (4th Cir. 2002). These cases discuss the application of the common law tort of negligent enablement of imposter fraud, a theory of liability that has met with mixed success in the courts, but should still be considered a viable possibility.

[12] *The Detection, Investigation, and Deterrence of Mortgage Loan Fraud Involving Third Parties: A White Paper*, Produced by the October 27, 2003 FFIEC Investigations Symposium, Issued February 2005.

a SAR report is generally triggered where there is actual or attempted perpetration of an act constituting a violation of federal criminal law (e.g., mortgage fraud, identity theft fraud, etc.), against or through a financial institution where the suspicious transaction involves at least $5,000, or where an insider is involved regardless of the dollar amount involved.[13] The following points should be considered when handling and processing SAR reports:

- **Institutions should designate one individual or department to be responsible for completing and filing SAR reports:** Where different departments or divisions within an institution file SAR reports separately, there is increased risk that SAR reports will not be filed under the institution's uniform Bank Secrecy Act (BSA) compliance program, that SAR reports might be inconsistent or incomplete, and that SAR reports could be duplicative.

- **Confidentiality of SAR reports:** Under most circumstances, the disclosure of the existence of a SAR report is prohibited, and doing so may constitute a violation of federal criminal law – thus possibly requiring the filing of another SAR report. In particular, care should be taken when preparing and filing the SAR report to ensure that the target of the filing is not informed of its existence. This can be difficult where the target is a senior executive officer of the institution.

- **Responding to requests for SAR reports:** Institutions should exercise caution in responding to requests for production of a SAR report. Most courts and regulatory interpretations have held that public disclosure of a SAR report is absolutely prohibited. Institutions should consult with bank regulatory counsel to confirm the application of SAR regulations to the specific circumstances of a request for production.

Where suspected mortgage fraud involves third parties, the regulators suggest that institutions contact the appropriate state licensing board (e.g., state appraiser or real estate licensing authorities).

Responding to Suspicion of Fraud Where Proof Does Not Exist

As part of their internal fraud detection and response programs, financial institutions are increasingly considering their options where they suspect that fraud may be involved in an application, but they do not have documentary evidence of the suspected fraud.

Under regulations promulgated by the Federal Reserve Board in Regulation Z, a creditor on a home equity plan may terminate the plan and demand repayment of the entire outstanding

[13] 12 C.F.R. § 21.11 (Office of the Comptroller of the Currency); 12 C.F.R. § 563.180 (Office of Thrift Supervision); 12 C.F.R. § 208.62 (Federal Reserve Board); 12 C.F.R. Pt. 353 (Federal Deposit Insurance Corporation).

balance in advance of the original term if there is fraud or material misrepresentation by the consumer in connection with the plan.[14] This provision, however, only applies to fraud on the part of the consumer, not to fraud perpetrated by a third party exclusive of the consumer. Regardless the source of the suspected fraud, financial institutions have certain obligations under the Fair Credit Reporting Act ("FCRA"), and the Equal Credit Opportunity Act ("ECOA") with respect to taking "adverse actions" against consumers. Under the FCRA, a financial institution can reject an applicant where it suspects fraud based on information contained in a consumer report, however as such constitutes an "adverse action," the institution is required by FCRA to inform the affected consumer of the source of the information and of the consumer's right to contest the accuracy of the information contained in the consumer report. Similarly, the ECOA requires that where an applicant is denied a mortgage loan, the denying institution must provide a statement as to the "specific reasons" for the denial.[15]

Where the institution lacks specific indicia of fraud, taking an adverse action against a consumer based on suspicion of fraud creates definite risks for the institution. Where financial institutions choose to take an adverse action against an applicant or existing customer based on suspicion of fraud, such institutions should be mindful of the following attendant risks: regulatory risk, litigation risk, reputation risk, and safety and soundness risk. Some of the more common adverse actions that would trigger these risks include: rejection of the applicant, assessment of a default rate of interest, suspension of access to the account, set-off against funds, and closure of the account.

Conclusion

Mortgage fraud, and identify theft in furtherance of mortgage fraud, are equal opportunity crimes – they can affect community banks and large banks. The attendant risks and costs of mortgage fraud reach beyond mere loss on a loan; financial institutions that are the victims of mortgage fraud due to deficient internal controls and prevention and response procedures, may suffer regulatory, litigation, and reputational consequences. In conducting their regular self-assessments of their fraud response programs, institutions should consider not only existing threats, but also the innovative schemes that potential fraudsters are constantly planning. Institutions should constantly identify and monitor potential weaknesses in their fraud prevention defenses – because surely the perpetrators of fraud are doing so.

[14] 12 C.F.R. § 226.5b(f)(2)(i) (2007).

[15] 15 U.S.C. § 1691.