Mortgage Fraud and Data Breaches

William Purce

Director of Mortgage Regulation

MORTGAGE FRAUD

Primary Forms of Mortgage Fraud

Mortgage fraud takes two primary forms: Fraud for Profit and Fraud for Housing.

Fraud for Profit usually involves industry insiders such as appraisers, brokers, and loan originators. Such schemes aim to gain cash or home equity through abuse of the mortgage lending process.

Fraud for Housing primarily consists of illegal actions by borrowers motivated to acquire or maintain ownership of a home.

Types of Mortgage Fraud

- **Income Fraud:** Inflating income to qualify for larger loans.
- **Employment Fraud:** Falsifying employment details.
- **Occupancy Fraud:** Claiming owner-occupancy for better loan terms.
- **Appraisal Fraud:** Inflated property values via collusion.
- **Straw Buyer Schemes:** Using another person’s identity to secure a loan.
- **Identity Theft:** Using stolen identities to obtain mortgages.
- **Property Flipping (Illegal):** Buying low, inflating value, and reselling quickly.
- **Non-Arm’s Length Transactions:** Deals between related parties to manipulate terms.

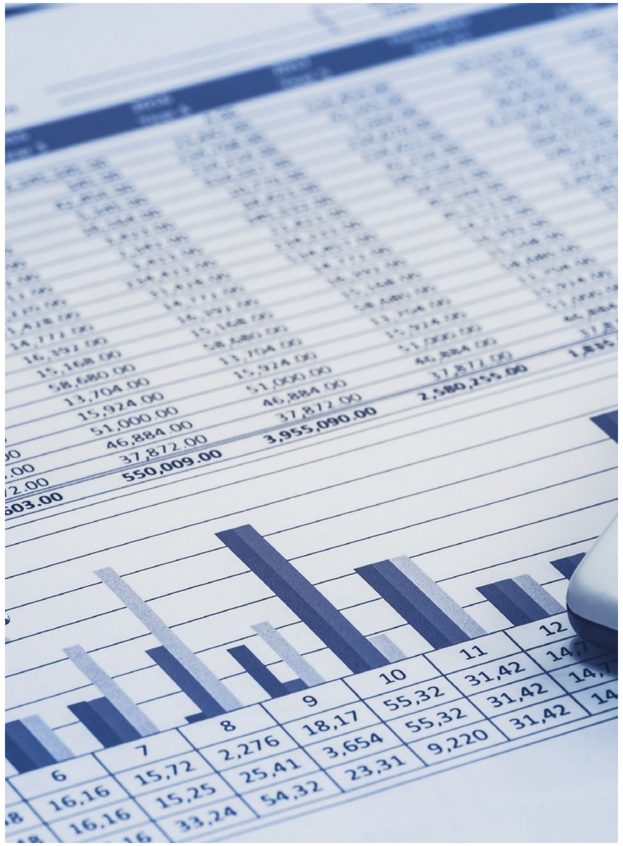
Types of Mortgage Fraud (fraud committed by mortgage professionals)

Air Loans – An air loan is a loan made based on fictitious collateral. To make air loans, broker may invent fake borrowers and properties, establish accounts for payments, and maintain custodial accounts for escrows. They may establish fraudulent contacts for fictitious employers, appraisers, credit agencies, and others to deceive creditors who attempt to verify information on loan applications.

Appraisal – Appraisal fraud is committed when a property is fraudulently valued either above or below its true market value. Appraisal fraud may occur as a result of efforts to ensure that a property's value appears consistent with an agreed purchase price, permitting the transaction to move forward, but fraudsters also commit appraisal fraud in order to profit from the difference in the fraudulent and true property values in a subsequent transaction.

Shotgunning – Shotgunning fraud aims to secure multiple loans on a single property from different financial institutions without each other's knowledge. Possible at both the purchase or refinancing stages, the fraudster aims to receive the loan disbursements simultaneously, then abscond with the proceeds, leaving the lenders to allocate losses and determine who holds the collateral.

Real Estate Owned (REO) Fraud – REO fraud occurs after a property has entered the foreclosure process, and the financial institution which took the property as collateral must maintain, market, and sell the home to recoup losses from the unpaid mortgage. Fraudsters may take advantage of this stage through a variety of schemes such as fraudulent billing for fictitious maintenance charges, kickbacks arranged through non-arm's length transactions, and laying the groundwork for flipping or flopping schemes.



Different Types of Occupancy Fraud

Three different types of occupancy fraud:

- **Classic Occupancy Fraud:** Borrowers claim they will occupy the property as their primary residence when they actually plan to use it for investment or rental purposes.
- **Straw Buyer Fraud:** A borrower uses another person (the "straw buyer") with good credit to obtain a mortgage on their behalf, while the actual occupant is someone else.
- **Reverse Occupancy Fraud:** A borrower purchases a home as an investment property and claims rental income to qualify for the mortgage loan but instead of renting the property, the borrower occupies the property as a primary residence.

Mortgage Fraud – Violation of State Law

Section 32.32 of the Texas Penal Code indicates that mortgage fraud is committed if a person intentionally or knowingly makes a materially false or misleading written statement to obtain a mortgage loan.

> (b) A person commits an offense if he intentionally or knowingly makes a materially false or misleading written statement to obtain property or credit, including a mortgage loan.
>
> (b-1) A person commits an offense if the person intentionally or knowingly makes a materially false or misleading written statement in providing an appraisal of real property for compensation.

Required Fraud Notice to Borrower

As part of a home loan transaction, a person (the borrower) must sign a Notice of Penalties for Making False or Misleading Written Statement at closing. See [Section 343.105 of the Texas Finance Code]. The actual notice reads as follows:

> "Warning: Intentionally or knowingly making a materially false or misleading written statement to obtain property or credit, including a mortgage loan, is a violation of Section 32.32, Texas Penal Code, and, depending on the amount of the loan or value of the property, is punishable by imprisonment for a term of 2 years to 99 years and a fine not to exceed $10,000.
>
> "I/we, the undersigned home loan applicant(s), represent that I/we have received, read, and understand this notice of penalties for making a materially false or misleading written statement to obtain a home loan.
>
> "I/we represent that all statements and representations contained in my/our written home loan application, including statements or representations regarding my/our identity, employment, annual income, and intent to occupy the residential real property secured by the home loan, are true and correct as of the date of loan closing."

Mandatory Reporting of Mortgage Fraud

Section 402.033 of the Texas Government Code establishes the reporting requirements for reporting suspected mortgage fraud to an authorized government agency. Specifically, Section 402.033(b) of the Texas Government Code reads as follows:

> "If a person determines or reasonably suspects that fraudulent activity has been committed or is about to be committed, the person shall report the information to an authorized governmental agency. If a person reports the information to the attorney general, the attorney general shall notify an appropriate law enforcement agency with jurisdiction to investigate the fraudulent activity. If a financial institution or person voluntarily or pursuant to this section reports fraudulent activity to an authorized governmental agency, the financial institution or person may not notify any person involved in the fraudulent activity that the fraudulent activity has been reported, and the authorized governmental agency who has any knowledge that such report was made shall not disclose to any person involved in the fraudulent activity that the fraudulent activity has been reported. Any financial institution or person that makes a voluntary report of any possible violation of law or regulation to an authorized governmental agency shall not be liable to any person under any law or regulation of the state or the United States for such report."

SML Recent Experience with Fraud Cases

- Mortgage fraud referral from Academy Mortgage Corporation
- The residential mortgage originator – Sophia Perez (NMLS ID 324884) - created false documents:
  - 24 loans - false or fraudulent Social Security Administration "Benefit Verification Letters"
  - 8 loans - false or fraudulent bank statements
  - 4 loans - false or fraudulent "Verification of Rent" forms
  - 4 loans – false or fraudulent utility bills
- SML investigated the mortgage fraud and reviewed mortgage loan files from some of the seven mortgage entities that employed Ms. Perez over a three-year period.
- Outcome – Revocation of RMLO license – 04/29/2025

SML Recent Experience with Fraud Cases

- Mortgage fraud referral from Federal Housing Finance Agency
- Residential mortgage originator – Kimberli Tomman (NMLS ID 222287).
- On or about February 15, 2023, Kimberli Tomman was indicted on federal charges of: (1) conspiracy to make false statements to mortgage lending businesses and financial institutions (18 U.S.C. § 371); and (2) aiding and abetting false statements to a mortgage lending business (18 U.S.C. § 1014).
- Ms. Tomman forged a death certificate to allow a straw buyer's spouse to indicate that the borrower was no longer responsible for further alimony payments.
- Outcome – Notice of Suspension of License – May 16, 2023, and Agreement to Surrender License on July 26, 2023. On October 28, 2025, pleaded guilty to the criminal offenses.

SML Recent Experience with Fraud Cases (pending)

- Mortgage fraud referral from a mortgage banker
- Nature of Misconduct: Fraudulent collection of funds for unperformed "credit repair" services by an MLO acting without legal authority
- Amount Collected: ~$11,540 via Apple Pay (seven possible accounts)
- Timeframe: May 2024 – September 2025
- Method: Over 400 text messages soliciting payments; used personal phone and Apple Pay
- False Claims:
  - Promised 80–100 point credit score increases
  - Claimed services were "almost complete" but performed no substantive work
  - MLO stated he was "not a credit repair company," but helping "as a courtesy"
  - MLO not registered and bonded as a credit services organization under Tex. Fin. Code, Ch. 393
  - No written contract for the purchase of the services of a credit service organization
  - Done without the knowledge or consent of MLO's sponsoring entity

SML Recent Experience with Fraud Cases (pending)

- Nature of Alleged Misconduct: Fraudulently billed Medicare for $4.5 million in COVID-19 test kits. Obtained $1.97 million by sending kits to individuals who never requested them — including deceased patients. Paid $488,435 in illegal kickbacks to acquire Medicare patient data.
- Alleged Violations (see table)
- Conduct unrelated to mortgage origination activity
- Outcome: MLO surrendered his TX-SML license.

Code Section	Offense Description
Title 18 U.S.C. Section 371	Conspiracy to commit offense or to defraud United States
Title 18 U.S.C. Section 1343	Wire Fraud
Title 18 U.S.C. Section 1516	Obstruction of a Federal Audit

SML Recent Experience with Fraud Cases (pending)

- Fraud referral from Federal Housing Finance Agency (FHFA)
- Nature of Alleged Misconduct: Bank and wire fraud scheme targeting the Paycheck Protection Program (PPP), a program created to address the economic fallout of the COVID-19 pandemic by providing forgivable loans to small businesses.
- Amount Collected: 22 PPP loan applications seeking a total $9.4 million in loan funds ($6.5 million was funded).
- Alleged Violations (see table)
- Conduct unrelated to mortgage origination activity
- Criminal complaint filed. SML monitoring status of indictment.

Code Section	Offense Description
Title 18 U.S.C. Section 1014	False Statements to a Financial Institution
Title 18 U.S.C. Section 1343	Wire Fraud
Title 18 U.S.C. Section 1344	Bank Fraud
Title 18 U.S.C. Section 1349	Conspiracy to Commit Wire Fraud
Title 18 U.S.C. Section 1957	Engaging in Prohibited Monetary Transactions

Common Red Flags for Income Fraud

(FHFA Common Flags)

Applicant's job title is generic, e.g., "manager," "vice president."	Employer's address is a post office box, the property address, or applicant's current residence.	Applicant's residence is (will be) in location remote from employer.	Employer name is similar to a party to the transaction, e.g., uses the applicant's initials.	Employer unable to be contacted.	Year-to-date or past-year earnings are even dollar amounts.
Withholding not calculated correctly (check FICA tables).	Withholding totals vary significantly from pay period to pay period.	Pay period dates overlap and/or do not correspond with other documentation.	Abnormalities in paycheck numbering.	Handwritten VOE, pay stubs, or W-2 form.	W-2 form presented is not the employee's copy.
Employer's identification number has a format other than 12-3456789.	Income appears to be out of line with type of employment.	Self-employed applicant does not make estimated tax payments.	Real estate taxes or mortgage interest claimed, but no ownership of real property disclosed.	Tax returns not signed or dated.	High-income applicant without paid preparer.
Paid preparer signs taxpayer's copy of tax returns.	Interest and dividend income do not align with assets.	Applicant reports substantial income but has no cash in bank.	Large increase in housing expense.	Reasonableness test: income appears to be out of line with type of employment, applicant age, education, and/or lifestyle.	

Common Red Flags for Occupancy Fraud
(FHFA Common Flags)

- Real estate listed on application, yet applicant is a renter.
- Applicant intends to lease current residence.
- Significant or unrealistic commute distance.
- Applicant is downgrading from a larger or more expensive house.
- Sales contract is subject to an existing lease.
- Occupancy affidavits reflect applicant does not intend to occupy.
- New homeowner's insurance is a rental policy (declarations page).
- Rental property listed on application is more expensive than subject property.
- Different mailing address on applicant's bank statements, pay advices, etc.
- Different address reported on credit report.
- Appraisal reflects vacant or tenant occupancy.
- Homeowner's insurance is a rental policy (declarations page).
- Reverse directory does not disclose subject property address.

Mortgage Fraud Resources

- FHFA Fraud Prevention: fhfa.gov
- CFPB Mortgage Compliance: consumerfinance.gov
- Fannie Mae Fraud Guide: selling-guide.fanniemae.com
- HUD Stop Loan Modification Scams: Prevent Loan Scams | HUD.gov / U.S. Department of Housing and Urban Development (HUD)

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

HECTOR RETTA, COMMISSIONER

DATA BREACHES

Reported Data Breaches (Texas)

REPORTED DATA BREACHES (Source: Texas Office of the Attorney General) (Section 521.053 of the Texas Business & Commerce Code)		
Fiscal Year (09/01 to 08/31)	Number of Mortgage Entities licensed or registered with TX-SML or related entity reporting a data breach involving 250 or more Texans	Number of affected Texas residents
FY2022	10	403,730
FY2023	3	125,319
FY2024	11	2,909,231
FY2025	5	11,063
FY2026YTD	3	24,585

Case Study 1

- **Root Cause:** Social engineering of Help Desk
- **Attack Vector:** Phone-based impersonation
- **Sequence of Events:**
  - Threat actor called the Help Desk late at night.
  - Used social engineering to impersonate a privileged IT staff member.
  - Help Desk reset the password for the impersonated account (only needed Social Security Number for the reset).
  - The attacker used the new credentials to access LogMeIn via Single Sign-On.
  - Access was granted because the attacker used a trusted IP (Zscaler) recognized by Microsoft Entra ID.
- **Lessons Learned:**
  - Help Desk training is critical to detect social engineering.
  - Conditional access rules should not blindly trust IPs.
  - Privileged accounts need stronger verification for password resets.

Case Study 2

- **Root Cause:** Abuse of trusted IP and weak MFA enforcement
- **Attack Vector:** Trusted IP bypassed Multifactor Authentication (MFA)
- **Sequence of Events:**
  - Compromised telephones via a third-party cellular carrier (MFA login credentials were re-routed to the threat actor)
  - Attacker accessed LogMeIn from a trusted IP.
  - Conditional Access rules allowed access without MFA.
  - Once inside, attacker performed reconnaissance on admin accounts.
  - Created new admin accounts and exfiltrated customer data.
  - Used virtual machines to bypass data loss prevention (DLP) programs and blend into admin traffic.
- **Lessons Learned:**
  - MFA should be enforced regardless of IP trust.
  - Monitor for unusual admin activity and virtual machine creation.
  - DLP systems must detect data movement within virtual environments.

Case Study 3

- **Root Cause:** Exploitation of ConnectWise ScreenConnect vulnerability
- **Attack Vector:** Known software vulnerability
- **Sequence of Events:**
  - Threat actor exploited a vulnerability in ConnectWise (same day as the vulnerability was discovered and released to the public).
  - Gained access to internal devices.
  - Exfiltrated data for extortion purposes.
  - No ransomware or encryption was used.
- **Lessons Learned:**
  - Patch management is essential.
  - Monitor for exploitation of remote access tools.
  - Check for known exploited vulnerabilities.
  - Even non-encrypting attacks can lead to data loss and extortion.

Case Study 4

- **Root Cause:** Phishing or brute force attack

  Brute force entry refers to a method where unauthorized individuals attempt to gain access to systems or data by systematically testing numerous combinations of credentials or encryption keys until the correct one is found. This method relies on trial and error and is often automated to quickly test a wide range of combinations.
- **Attack Vector:** Unclear (likely credential-based)
- **Sequence of Events:**
  - Threat actor gained access to servers.
  - Entry method suspected to be phishing or brute force.
- **Lessons Learned:**
  - Implement brute force detection and timeout/lockout mechanisms.
  - Use phishing-resistant MFA.
  - Investigate and log all failed login attempts.

Case Study 5

- **Root Cause:** Compromised self-service password reset
- **Attack Vector:** Exploitation of internal password reset tool
- **Sequence of Events:**
  - Attacker used the self-service password reset mechanism.
  - Gained unauthorized access to systems.
  - Mechanism was disabled after discovery.
- **Lessons Learned:**
  - Self-service tools must have strong identity verification.
  - Monitor for unusual password reset activity.
  - Disable all self-service password resets for privileged accounts.

Case Study 6

- **Root Cause:** Spear phishing and email account hijacking
- **Attack Vector:** Email from compromised third party
- **Sequence of Events:**
  - Loan officer received a spear phishing email from a known builder contact.
  - Loan officer entered Office 365 credentials and approved MFA from phishing email.
  - Attacker gained full access to email.
  - Implemented a soft token and modified mailbox rules to hide activity.
  - Security Operations Center (SOC) detected abnormal email traffic (584 outbound emails).
- **Lessons Learned:**
  - Train users to recognize phishing—even from known contacts.
  - Monitor for abnormal email behavior and mailbox rule changes.
  - Use phishing-resistant MFA (e.g., FIDO2 keys).

Case Study 7

- **Root Cause:** Exploited SonicWall CVE (CVE-2024-40766)
  - There are several reported vulnerabilities – CVE-2024-53704, 53705 and 53706.
- **Attack Vector:** Perimeter firewall vulnerability
- **Sequence of Events:**
  - Attacker used stolen credentials or exploited a SonicWall CVE.
  - Gained access to the network perimeter.
  - Deployed “Fog” ransomware.
  - Forensic analysis showed access to 10 systems over 3 days.
- **Lessons Learned:**
  - Monitor Common Vulnerabilities and Exposures (CVE) databases
  - Patch critical systems immediately.
  - Segment networks to limit lateral movement.
  - Use intrusion detection systems to catch early signs of compromise.

Cybersecurity Mitigation of Risk Strategy

Develop an Information Security Plan required by FTC Safeguards Regulation, 16 C.F.R. §314.4

1. **Designate a Qualified Individual**
   Appoint someone responsible for overseeing and implementing the information security program.
2. **Conduct a Risk Assessment (A written assessment is required if your business has 5,000 or more customers nationwide.)**
   Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.
3. **Design and Implement Safeguards**
   Based on the risk assessment, implement safeguards to control the identified risks. This includes access controls, encryption, secure development practices, and multi-factor authentication.
4. **Monitor and Test Safeguards**
   Regularly test or monitor the effectiveness of your safeguards. Continuous monitoring is preferred, but periodic testing is acceptable if continuous monitoring isn't feasible.
5. **Train Staff**
   Provide security awareness training to employees and update it as necessary to reflect risks and changes in the program.
6. **Monitor Service Providers**
   Take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards, and require them by contract to implement and maintain such safeguards.
7. **Keep Your Program Current**
   Evaluate and adjust your information security program in light of changes to your operations or the results of testing and monitoring.
8. **Create a Written Incident Response Plan (A written plan is required if your business has 5,000 or more customers nationwide.)**
   Develop a plan to respond to and recover from any security event that materially affects the confidentiality, integrity, or availability of customer information.
9. **Report to the Board of Directors or Oversight Committee**
   The Qualified Individual must provide a written report, at least annually, to the board of directors or equivalent governing body. This report should cover the overall status of the information security program and compliance with the Safeguards Rule.

Cybersecurity Mitigation of Risk Strategy

- **Create an IT/IS Governance Policy** based on a standard such as NIST 800-53: Security & Privacy Controls for Information Systems and Organizations
- **Develop and maintain a risk assessment that includes**:
  - an asset identification (hardware, software, and cloud resources)
  - a risk identification based on threats applicable to your business
  - a risk assessment and measurement tool that analyzes the likelihood, impact, and severity of the risk
  - a risk mitigation process that identifies and prioritizes ways to reduce risks and describe how the identified risks will be mitigated or accepted
  - identifies controls to mitigate or reduce risks
  - a risk monitoring process (internal, IT audits, or third-party vendor analysis)

Cybersecurity Mitigation of Risk Strategy

- **Create and maintain:**
  - an acceptable user policy that adequately outlines what activities are permitted and prohibited by employees
  - a data destruction/disposal plan that explains when and how records are to be destroyed
  - a data classification policy and procedure (sensitive, confidential, and public)
  - a software and hardware asset management program that address hardware inventory, software inventory, cloud assets, patching, end-of-life, configuration management, license management, procurement and development, and monitoring.
  - a vendor management program
  - a user access program that controls who has access to systems, removal or termination of employees, and modification of employee roles
  - a business continuity and disaster recovery plan
  - an incident recovery plan
  - a change management program
  - a mobile device management plan including “bring your own device”

Cybersecurity Mitigation of Risk Strategy

- **Implement or use:**
  - Firewall
  - Anti-virus programs
  - Multifactor Authentication (MFA)
  - Virtual private networks (VPNs) when accessing records remotely
  - Secure wireless router connections (change default name and password and turn off remote management)
  - Encryption
  - Strong, complex and unique passwords (password managers are acceptable)
  - Secure Sockets Layer (SSL) or other secure connection especially online credit applications
  - Security Information & Event Management (SIEM)
  - Role-based Access Controls especially for administrator accounts
  - Secure platforms to upload customer records

Cybersecurity Mitigation of Risk Strategy

- **Employee Training Program** – Employees should be periodically trained to:
  - follow your company's information security plan;
  - identify phishing or other cybersecurity attacks;
  - lock rooms and file cabinets where records are kept;
  - not share or openly post passwords in work areas;
  - only share non-public personal information with the employees that need the information to perform their duties;
  - encrypt sensitive customer information when it is transmitted electronically via public networks;
  - dispose of records in a proper method (record retention and destruction policy);
  - refer calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
  - report suspicious attempts to obtain customer information to designated personnel.

Mortgage Cybersecurity/IT Resources

- CSBS: Baseline Nonbank Cybersecurity Exam Program V1.1.pdf
- CSBS: Enhanced Nonbank Cybersecurity Exam Program V1.1.pdf
- FTC Safeguards Rule: What Your Business Needs to Know | Federal Trade Commission
- Start with Security: A Guide for Business | Federal Trade Commission
- SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC
- CVE: Common Vulnerabilities and Exposures

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
HECTOR RETTA, COMMISSIONER

Reportable Incidents

Definition of a Reportable Incident

- "Reportable incident" means an incident or situation that presents a material risk, financial or otherwise, to a mortgage entity's operations or its customers. A reportable incident includes the following items, provided, it presents a material risk:
  - (A) a "catastrophic event"; or
  - (B) a "security event".

Other Definitions

- "Catastrophic event" means an event, other than a security event, that is unforeseen and results in extraordinary levels of damage or disruption to operations (e.g., the destruction of a principal office or data center).
- "Security event" means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form. It includes information that is encrypted, if the person with unauthorized access to the information can decrypt the data.

Incident Report

- Within 30 days after the date the mortgage company/banker/servicer becomes aware of a reportable incident, the entity must submit a written incident report to SML.
- The incident report must include:
  - a detailed description of the nature and circumstances of the reportable incident;
  - the number of Texas residents affected or potentially affected by the reportable incident;
  - the measures taken by the mortgage banker/company/servicer to resolve or address the reportable incident;
  - the measures the mortgage banker/company/servicer plans to take to resolve or address the reportable incident; and
  - the point of contact designated by the mortgage banker for inquires by SML about the reportable incident.

Incidents Reported to Other Agencies

- The notification requirement shown on the previous slide is satisfied if SML receives the same notification sent to:
  - the Federal Trade Commission (FTC) required by Section 314.4(j) of the FTC's Standards for Safeguarding Customer Information rules (16 C.F.R. §314.4(j)); or
  - the Office of the Attorney General of Texas required by Business and Commerce Code §521.053(i).

Root Cause Analysis for Security Events

- Within 120 days after the mortgage company/banker/servicer becomes aware that a security event has occurred, the mortgage entity must provide SML with a root cause analysis report of the security event.
- "Root cause analysis report" means a written report concerning the results or findings of an audit or investigation to determine the origin or root cause of a security event, identify strategic measures to effectively contain and limit the impact of a security event, and to prevent a future security event.

Supplemental Information

- SML may require additional, clarifying, or supplemental information or documentation related to a reportable incident as SML deems necessary or appropriate.
- Any information including the root cause analysis report and supplemental information is confidential examination/inspection information.

Questions?

William Purce
Director of Mortgage Regulation
(512) 936-6602
wpurce@sml.texas.gov