

INTRODUCTION.....	2
SUSPICIOUS ACTIVITY REPORTS.....	2
Filing Suspicious Activity Reports.....	2
Reporting Timeframes.....	2
Record Retention.....	3
Board Reporting.....	3
Confidentiality.....	3
Safe Harbor Provision.....	3
THE ROLE OF EXAMINERS.....	3
Notification Prohibition.....	4
INTERAGENCY COOPERATION.....	4
Communication and Points of Contact.....	4
Referrals to the Department of Justice (DOJ).....	4
ASSISTANCE TO LAW ENFORCEMENT.....	4
Parallel Proceedings.....	5
FEDERAL GRAND JURY SUBPOENAS.....	5
SAFEGUARDING EVIDENCE.....	5
BONDING COMPANY NOTIFICATION.....	6
OTHER MATTERS.....	6
CRIMINAL STATUTES.....	6
SIGNIFICANT CIVIL STATUTES.....	13

INTRODUCTION

Criminal conduct and fraudulent acts undermine public confidence in the financial system and contribute to financial institution failures. Confidence is especially eroded when offenses involve bank insiders. When failures occur, the FDIC deposit insurance fund can suffer significant losses.

If allegations or evidence of wrongdoing comes to the FDIC's attention, a prompt response is warranted. The scope of a response varies based on the severity and specificity of allegations and the reliability of corroborating evidence. Examiner discretion, sound judgment, and regional office coordination are needed to appropriately respond to indications of improper conduct or fraudulent acts.

The primary responsibility for preventing, detecting, and reporting fraud and insider abuse rests with a bank's board of directors and senior management. Early detection and reporting of suspicious activities is in a bank's best interest as it can reduce liabilities resulting from operational errors and may limit or prevent monetary losses. The board must establish appropriate internal controls and effective audit programs to fulfill their legal and fiduciary duties. Controls and safeguards should address internal and external offenses and include procedures for identifying and reporting suspicious activities. Financial institutions must report questionable actions using a Suspicious Activity Report (SAR).

←

SUSPICIOUS ACTIVITY REPORTS

Part 353 of FDIC Rules and Regulations and CFR¹ Title 31, Chapter X, § 1020.320 of the Financial Crimes Enforcement Network (FinCEN) regulations require insured nonmember banks and state chartered savings associations to report suspicious activities to FinCEN, a bureau of the U.S. Department of the Treasury. The primary purpose of the reporting requirement is to ensure investigators and prosecutors are provided relevant information in an orderly and timely fashion. Financial institutions must report suspicious activities on electronically filed SARs, which allow law enforcement and regulatory agencies to more efficiently assess and respond to questionable actions.

¹ The U.S. Code of Federal Regulations (CFR) is the codification by subject matter of the general and permanent laws of the United States. It is divided by broad subjects into 50 titles and published by the Office of the Law Revision Counsel of the U.S. House of Representatives.

Filing Suspicious Activity Reports

A financial institution is required to file an SAR when it detects a known or suspected criminal violation of federal law, a suspicious transaction related to potential money laundering, or a violation of the Bank Secrecy Act (BSA). Banks should file SARs with appropriate federal law enforcement agencies and the Department of the Treasury in accordance with the report's instructions. Generally, completed SARs should be transmitted to FinCEN in the following circumstances:

- Insider abuse² involving any amount when the financial institution believes it is either an actual or potential victim of a committed or attempted criminal transaction and the financial institution has identified a director, officer, employee, agent, or other institution-affiliated party as having committed or aided in the commission of the criminal act;
- Transactions aggregating \$5,000 or more in funds or other assets when a suspect can be identified and the financial institution believes it is either an actual or potential victim of a committed or attempted criminal transaction;
- Transactions aggregating \$25,000 or more in funds or other assets regardless of potential suspects and the financial institution believes it is either an actual or potential victim of a committed or attempted criminal transaction; or
- Transactions aggregating \$5,000 or more that involve potential money laundering or violations of the BSA.

Note: Financial institutions are not required to file an SAR for a robbery or burglary committed or attempted that is appropriately reported to law enforcement authorities.

Reporting Timeframes

Financial institutions are required to file SARs no later than 30 calendar days after the date of the initial detection of facts that constitute the basis for filing an SAR. An institution may delay filing an SAR for an additional 30 calendar days to identify a suspect. However, in no case should institutions delay reporting more than 60 calendar days after the date of initial detection of a reportable transaction. Further, in situations involving violations that require immediate attention, such as ongoing money

² Insider abuse may involve known or suspected criminal violations of federal law committed by an insider against a bank customer involving a transaction or transactions facilitated by or through the bank.

laundering activities, the financial institution should immediately notify an appropriate law enforcement authority by telephone in addition to promptly filing an SAR. Refer to Part 353 and CFR Title 31, Chapter X, § 1020.320(b) for additional details.

Record Retention

Financial institutions must maintain a copy of any SAR filed and the original, or business record equivalent, of any supporting documentation for a period of five years from the date of filing. Supporting documentation identified and maintained by the financial institution as such, will be deemed to have been filed with the SAR. The financial institution must make all supporting documentation available upon request to FinCEN, appropriate law enforcement agencies, and state or federal regulatory authorities that examine the bank for compliance with the BSA.

Board Reporting

Management is required by Part 353 to promptly notify its board of directors, or a committee thereof, of any SAR filed. In addition, the board should record such notification in its minutes.

Confidentiality

Suspicious activity reports are confidential. Any institution subpoenaed or otherwise asked to disclose an SAR or related information shall decline to produce the SAR or provide any information indicating an SAR was prepared or filed. Institutions should notify their FDIC regional office of any such requests.

Additionally, neither the financial institution, nor its current or former directors, officers, employees, agents, or contractors may notify any person involved in a transaction that an SAR was filed or disclose any information that would reveal the existence of an SAR.

Safe Harbor Provision

In general, financial institutions and their directors, officers, employees, and agents are protected from civil liability for filing SARs and for failing to provide notice of such filings to individuals named in the SARs. Refer to CFR Title 31, § 5318(g) for additional information.

←

THE ROLE OF EXAMINERS

Examiners should consider the adequacy of internal controls at each examination and remain alert for suspicious or unusual activities during each functional review. If examiners identify or become aware of questionable conduct or transactions, they should discretely investigate their concerns and discuss the issues with the examiner-in-charge and field or regional office personnel. Examiners should securely retain documentation of transactions, discussions with management (or other bank personnel) and any other pertinent information relating to their investigations. Explanations by bank personnel that appear unreasonable should not be accepted without being fully investigated; however, information that supports management's explanations should be clearly documented.

If material concerns remain after examiners complete their initial investigations, they must immediately notify field and regional office personnel. This is paramount when board members or senior managers are suspected of wrongdoing, or when losses attributable to the activity imperils the institution's continued operation.

Examiners must consult with the supervisory regional office before informing the institution's board of directors or anyone associated with the institution of the suspicious activity. Generally, (after consulting with the regional office) apparent criminal violations that are detected by examiners should be brought to management's attention. However, the examiner should only present facts and must not make any statements or insinuations regarding possible conclusions as to particular individuals.

Generally, examiners should discuss the requirements of Part 353 with bank officials. However, it may be inappropriate to notify the board of directors or management when senior financial institution officials are implicated in the suspicious activity, or if the examiner has reason to believe that an official might flee, warn the target, destroy evidence, or otherwise jeopardize an investigation.

Further, if the financial institution fails to file an SAR, examiners should report the financial institution's decision to the regional office. The regional office should then determine whether a SAR should be filed.

Under certain circumstances, examiners may need to collect information supporting an SAR and submit it directly to the regional office. These situations generally occur when the financial institution is unable to file an SAR without alerting the subject, unwilling to file an SAR on an insider, or unwilling to file an SAR when the activity may imperil the institution's continued operation. If the regional office agrees with the examiner's assessment, an SAR may be filed by regional office staff.

The fact that an SAR has been filed does not prevent the examiner from making a more detailed written report. If necessary, the examiner may need to gather facts to support corrective actions, which may include recommendations for removal and prohibition.

Notification Prohibition

Pursuant to Title 31, U.S.C. 5318(g)(2)(A), no current or former officer or employee of, or contractor for, federal, state, local or territorial government who has knowledge that an SAR was filed, may disclose that fact to any person involved in the transaction, except in fulfilling official duties.

←

INTERAGENCY COOPERATION

The FDIC, other federal banking regulators, and various other agencies have agreed to cooperate and exchange information when necessary to address suspicious activity affecting insured financial institutions.

Communication and Points of Contact

Procedures have been formalized for interactions between RMS and the Office of Inspector General - Office of Investigations (OIG) with respect to investigations involving operating institutions. If an examiner or other RMS staff member is contacted directly by law enforcement, they must report the contact through the appropriate channels to the RMS deputy regional director or designee, who will notify the OIG and the Legal Division. Furthermore, the transfer of FDIC documents or records requested by law enforcement must comply with 12 C.F.R. § 309.6 (Disclosure of Exempt Records). The OIG and the Legal Division will coordinate the transfer of such documents and records. The OIG may oversee the investigation and coordinate interviews of appropriate RMS employees or the review of documents. No RMS employee should communicate directly with law enforcement, without prior approval of regional management and the Legal Division. However, permission is not required when disclosure is made solely to the FDIC Office of Inspector General - Office of Investigations. Refer to the Right to Financial Privacy Act for more information.

Referrals to the Department of Justice (DOJ)

The referral of suspicious activity to the DOJ or various U.S. Attorney Offices does not restrict the FDIC from continuing its own research into the same activity.

However, the FDIC may cease or suspend such activity if requested to do so by the DOJ due to an ongoing criminal investigation or prosecution. In all cases, the FDIC should keep the DOJ or U.S. Attorney informed of the progress of any parallel civil investigation with a view toward reaching a cooperative solution. Such cooperation might lead to a demand for restitution and stipulation to a prohibition from future banking employment being included in a criminal plea agreement or pre-trial diversion arrangement.

←

ASSISTANCE TO LAW ENFORCEMENT

Examiners may be asked to provide expertise to law enforcement agents investigating suspicious activity or prosecuting a criminal case. Requests are usually made in connection with bank fraud or money laundering cases, and the assistance is often needed for the following reasons:

- To interpret subpoenaed documents obtained from the financial institution;
- To explain the flow or processing of documents;
- To determine whether acquired documents are relied upon by FDIC examiners, other regulators, auditors, or managers to formulate business decisions or opinions as to the condition of the financial institution;
- To provide information concerning banking policies or general banking practices; or
- To provide specific assistance, such as testifying at a trial or before a federal grand jury.

Examiners should cooperate to the fullest extent possible in honoring reasonable requests for assistance, and the regional office should supply examiners with specific guidance governing each assignment. A written agreement may be necessary for long-term assignments, and the following guidelines apply to most requests for examiner assistance:

- The request for assistance must be for a legitimate law enforcement purpose within the jurisdiction of the requesting agency;
- The information requested, or that which the examiner has been asked to review, must be relevant to a legitimate law enforcement inquiry;
- The suspicious activity should involve an FDIC-insured institution, its directors, officers, employees, agents or customers;
- Any known, potential respondents (employees, officers, directors, or other IAPs) resulting from an investigation should be identified in addition to naming the institution itself;
- Compliance with all applicable provisions of the Right to Financial Privacy Act covering disclosures of

information derived from financial institution customer records must be assured; and

- The examiner should be instructed that while assisting the law enforcement authorities, he or she will be acting solely as a representative of the law enforcement authority, will not represent the FDIC in any way, and should not assert or exercise any authority as an FDIC examiner.

Parallel Proceedings

Although administrative and criminal investigations may occur concurrently, they must remain separate, independent investigations. Maintaining independence is critical when conducting coordinated investigations. While a coordination of activities between investigations is acceptable, a lack of independence may result in the suppression of evidence and/or the dismissal of an indictment. Therefore, examiners should not accompany law enforcement agents onto a financial institution’s premises in order to collect records as it may create the appearance of a lack of independence between separate investigations.

←

FEDERAL GRAND JURY SUBPOENAS

A federal, grand jury subpoena is an investigatory tool used to build the prosecution's case without compromising the privacy of investigation targets or prematurely revealing their investigatory directions. Rule 6(e) of the Federal Rules of Criminal Procedure requires that grand jury proceedings be kept secret to the fullest extent practicable. Grand jury secrecy is maintained principally:

- To encourage witnesses to come forward and to testify freely and confidentially;
- To minimize the risks that prospective defendants will flee or use corrupt means to thwart investigations and escape punishment;
- To safeguard the grand jurors and proceedings from extraneous pressures and influences;
- To avoid unnecessary disclosures that may make individuals appear guilty of misconduct without their being afforded opportunity to challenge the allegations; and
- To prevent information given under compulsion and for purposes of public justice from being used for insubstantial purposes, such as gossip, to the detriment of the criminal justice system.

Rule 6(e)(3)(A)(iii) allows grand jury matters to be disclosed to government attorneys and banking regulators for enforcing civil forfeiture and civil banking laws

pursuant to 18 U.S.C. 3322. However, 18 U.S.C. 3322 requires that a person to whom a matter has been disclosed shall not use such matter other than for the purposes for which such disclosure was authorized. The term “banking law violation” means a violation of, or a conspiracy to violate, sections 215, 656, 657, 1005, 1006, 1007, 1014, 1344, 1956 or 1957 of Title 18; as well as any violation of section 1341 or 1343 affecting a financial institution; or any provision of subchapter II of Chapter 53 or Title 31.

FDIC management must make a determination as to allowing appropriate and sufficient RMS and legal staff access to grand jury information. Nevertheless, possession of grand jury documents or testimony requires great care in order to comply with the secrecy requirements of Rule 6(e) of the Federal Rules of Criminal Procedure.

The FDIC’s General Counsel has the delegated authority to authorize an examiner to appear and testify before the grand jury or at a criminal trial. The examiner may be directed to contact the prosecutor or investigator either before or after a grand jury subpoena is issued to assist in identifying and gathering documents pertinent to the investigation. The examiner will be provided with appropriate counsel before testifying.

←

SAFEGUARDING EVIDENCE

Copies of the SAR and all supporting evidentiary documents should be segregated and stored in the regional office to ensure that the documents are readily retrievable and can be provided to law enforcement officials if needed.

Examiners should consult the regional office regarding necessary documentation. Generally, copies of documents must be made during the examination. The copies should be initialed and dated by the examiner in case the originals are misplaced or destroyed.

In addition to electronically copied documents, the examiner should document the flow of funds, approvals, and employees responsible for handling each transaction. Flow charts or similar methods may be appropriate for documenting complex transactions.

The following questions provide examples of the line of inquiry an examiner may follow in deciding how to review and document a particular circumstance:

- What is the financial institution’s policy for handling this type of transaction?
- Was there deviation from the policy?
- Who was authorized to make this transaction?

- Who handled this transaction?
- Who had knowledge?
- Who benefited ultimately from the transaction?
- What knowledge did the financial institution’s directors have?
- What was the credit quality at the time of making a loan and what it is now?
- Was the documentation adequate at inception?
- Was collateral value adequate at inception?
- Are there presently any credit or legal problems?
- Is the financial institution facing possible risk or damage other than financial loss?

←
BONDING COMPANY NOTIFICATION

The FDIC and financial institution management have a mutual interest in ensuring that all of a financial institution’s employees are protected by a fidelity bond. When a financial institution files an SAR involving an employee, it normally is required to notify its fidelity insurer of the subject activity. However, a financial institution may not provide a copy of the SAR to the insurer.

The notification requirement is usually included in the terms of the insurance contract and is not dependent upon the filing of a claim against the insurance coverage. The standard financial institutions bond contains a termination clause that automatically cancels coverage of any employee as soon as there is knowledge of any dishonest or fraudulent act on the part of such employee. The insurer need not give notice of such termination; in fact, the decision of the insurer may be made at a subsequent date. In the rare case in which a financial institution official has knowledge of a suspicious act on the part of an employee, yet wishes to continue to employ that person, management should obtain either an assurance in writing from the insurer’s main office (agents generally are not so empowered) that such person is still covered under the bond, or obtain a new bond covering that person. Refer to the Manual Section 4.4, Fidelity and Other Indemnity Protection for additional information.

If an examiner becomes aware that an employee has or will be reported to the fidelity bond company for suspicious acts (whether coverage is terminated or not), the examiner should contact the regional office. The regional office and examiner should consider whether to commence an investigation of the employee’s acts to determine if removal and prohibition or other administrative action under section 8 is warranted.

←
OTHER MATTERS

Examiners that receive information about alleged misconduct by a financial institution, its officers, employees, or directors may be asked to protect the informant's identity. When this happens, the examiner should advise the informant that the FDIC will try to protect the identity of the informant. However, prior to receiving the information, the examiner should advise the informant of the following facts:

- Mere inquiry into the situation may allow the institution’s management or employees to deduce the informant's identity;
- The information may be referred to another agency, such as the Department of Justice, which may request the informant's identity to continue or complete an investigation; and
- If the information becomes the basis for a criminal prosecution, the court may order disclosure of the informant's identity to the defendant.

←
CRIMINAL STATUTES

United States Code Title 18 is applicable to many criminal or fraudulent acts relating to financial institutions. Several sections of Title 18 and other pertinent Titles that an examiner might encounter are described below.

Title 18 - Crimes and Criminal Procedure
Part I > Chapter 1 > § 2
Aiding and Abetting

Whoever aids, abets, counsels, commands, induces, or procures the commission of a federal offense is punishable as a principal.

18 U.S.C. § 4 - Misprision of Felony

This statute applies to a person who has knowledge of the actual commission of a felony but conceals the knowledge and does not report that knowledge to a judge or other person in civil or military authority. A financial institution that fails to report an offense of which it is aware can be charged with violating this section.

18 U.S.C. § 20 - Financial Institution Defined

The definition of financial institution was expanded under the Fraud Enforcement and Recovery Act (FERA) of 2009 to include a mortgage lending business or any person or entity that makes in whole or part, a federally related

mortgage loan as defined in the Real Estate Settlement Procedures Act (RESPA) of 1974. Under § 27, a mortgage lending business is defined to include an organization which finances or refinances any debt secured by an interest in real estate, including private mortgage companies and any subsidiaries, and whose activities affect interstate or foreign commerce. Prior to the amendment, only FDIC or NCUA insured institutions, Federal Home Loan Banks, Farm Credit System, uninsured foreign banks, and Federal Reserve member banks were considered financial institutions.

Chapter 11 - Bribery, Graft, and Conflicts of Interest

18 U.S.C. § 201 - Bribery of Public Officials

This statute bans the offering or soliciting of bribes to or by federal officials, elected representatives, jurors or witnesses in official proceedings with the intent to influence an official act, or to influence the public official to commit, aid in committing, collude in, or allow any fraud; or to induce the public official to omit to do any act in violation of his lawful duty.

18 U.S.C. § 215 - Bank Bribery

Anyone who corruptly gives, offers, or promises anything of value with the intent to influence or reward an officer, director, employee, agent, or attorney of a financial institution in connection with any business or transaction, or any financial institution official who corruptly solicits or demands such things of value, would violate this statute.

Financial institutions are encouraged to prohibit insiders from self-dealing or otherwise trading on their positions at the financial institution; or accepting from one doing or seeking to do business with the financial institution, a business opportunity not generally available to the public. In this regard, the financial institution's code of conduct or policies should require that its officials disclose all potential conflicts of interest, including those in which they have been inadvertently placed due to either business or personal relationships with customers, suppliers, business associates, or competitors of the financial institution.

It should be noted that this section does not apply to bona fide salary, wages, fees, or other compensation paid, or expenses paid or reimbursed, in the usual course of business.

Chapter 19 - Conspiracy

18 U.S.C. § 371 - Conspiracy to Defraud

This statute covers a conspiracy of two or more persons to commit a federal offense or to defraud the United States or any agency thereof. This statute has been cited when two or more persons willfully ignored the notice requirements of the Change in Bank Control Act.

Chapter 25 - Counterfeiting and Forgery

18 U.S.C. § 471 - Counterfeiting and Forgery (Counterfeit Deterrence Act of 1992)

This statute applies to persons who falsely make, forge, counterfeit, or alter any obligation or other security of the United States with intent to defraud.

18 U.S.C. § 472 - Counterfeiting and Forgery

This statute applies to persons who intentionally defraud, pass, utter, publish, or sell the items contained in § 471 above. It also includes those persons who attempt to do so, or those who keep in their possession or conceal any such items.

18 U.S.C. § 500 - Counterfeiting and Forgery - Money Orders

This statute applies to persons who intentionally defraud, falsely make, forge, counterfeit, engrave, or print any order in imitation of, or purporting to be, a blank money order. It also applies to those who receive or possess any such money order with the intent to convert it for their own use or gain, knowing that it had been embezzled, stolen, or converted.

Chapter 31 - Embezzlement and Theft

18 U.S.C. § 656 - Theft, Embezzlement, and Misapplication by Bank Officer or Employee

This statute prohibits the willful theft, embezzlement, or misapplication of financial institution funds by an officer, director, agent, or employee of a financial institution with the intent to injure or defraud the financial institution. For example:

- Loans granted by a financial institution officer to fictitious borrowers,
- Loans granted based on inadequate or valueless collateral if the loan officer benefited personally or acted in reckless disregard of the institution's interests, and
- Brokered loans where deposits are provided for a fee to fund a loan that is worthless from its inception.

18 U.S.C. § 657 - Theft, Embezzlement, and Misapplication of Funds

This statute requires that any officer, agent, or employee of, or connected in any capacity with the FDIC, et al., who embezzles, abstracts, purloins or willfully misapplies any moneys, funds, credits, securities, or other things of value belonging to an insured institution will be fined or imprisoned.

18 U.S.C. § 658 - Property Mortgaged or Pledged to Farm Credit Agencies

This statute applies to persons who intentionally defraud, knowingly conceal, remove, dispose of, or convert to their own use, or to that of another, any property mortgaged or pledged to, or held by, the Farm Credit agencies.

18 U.S.C. § 664 - Theft or Embezzlement from Employee Benefit Plans

This statute applies to persons who intentionally embezzle, steal, or unlawfully and willfully abstract or convert to their own use or to the use of another, any of the monies, funds, securities, premiums, credits, property, or other assets of any employee welfare benefit plan or employee pension benefit plan, or of any fund connected therewith.

18 U.S.C. § 667 - Theft of Livestock

This statute applies to those who market \$10,000 or more in livestock, in interstate or foreign commerce, with the intent to deprive another of a right to the property or a benefit of the property or to appropriate the property to his or another's use.

Chapter 33 - Emblems, Insignia, and Names**18 U.S.C. § 709 - False Advertising or Misuse of FDIC Name**

This statute covers false advertising or representations, misuse or unauthorized use of words such as national, reserve, federal deposit, or deposit insurance, or misuse of names such as FDIC, to convey the impression of federal agency affiliation.

Chapter 47 - Fraud and False Statements**18 U.S.C. § 1001 - False Statements or Entries**

This statute generally covers oral or written false statements that are knowingly or willingly made, or concealment of a material fact, for the purpose of influencing a determination of any federal department or

agency. It is not necessary to show that the governmental body was actually influenced thereby.

18 U.S.C. § 1005 - Bank Entries, Reports, and Transactions

This statute covers false entries and reports or statements, including material omissions, made by an officer, director, agent, or employee of an insured bank with intent to injure or defraud the bank, or to deceive the FDIC or other individuals or companies. This section also prohibits any such person from issuing or putting forth in circulation any notes of the bank or making, drawing, issuing, or assigning any certificate of deposit, draft, order, bill of exchange, acceptance, note, debenture, bond or other obligation, or mortgage, judgment or decree. The crime may be committed personally or by direction (e.g., an officer directing the making of false entries).

Examples:

- Actions taken by an officer or employee to conceal delinquencies or to disguise potential lending limit violations
- Recording securities transactions at other than market value to hide losses

18 U.S.C. § 1007 - Federal Deposit Insurance Corporation Transactions

This statute covers false statements made for the purpose of influencing an action of the FDIC in any way. This includes willfully over-valuing any security for the purpose of obtaining, extending, or renewing a loan and statements made to induce the payment of an insured deposit, the purchase of assets, or the payment of any claim by the FDIC. To establish a violation of this statute, it is not necessary to prove loss or damage to the FDIC caused by the falsification. Violations of this section occur when false statements are made to the FDIC in connection with an application for deposit insurance, notice to acquire control of an insured state nonmember bank, or other processes in which FDIC is required to take action. False or misleading statements made to an FDIC examiner during an examination are also covered.

18 U.S.C. § 1010 - Department of Housing and Urban Development (HUD) Transactions

This statute prohibits for the purpose of obtaining any loan or advance of credit from any person, partnership, association, or corporation with the intent that such loan or advance of credit will be offered to or accepted by HUD for insurance, or for the purpose of obtaining any extension or renewal of any loan, advance of credit, or mortgage insured by HUD, or the acceptance, release, or substitution

of any security on such a loan, or for the purpose of influencing in any way the action of HUD, by making, passing, uttering, or publishing any statement, knowing the same to be false, or altering, forging, or counterfeiting any instrument, paper, or document, or uttering, publishing, or passing as true any instrument, paper, or document, knowing it to have been altered, forged, or counterfeited, or willfully overvaluing any security, asset, or income, will be fined and/or imprisoned.

18 U.S.C. § 1014 - False Statements on a Loan or Credit Application

This statute covers any false statements or reports made knowingly on a loan or credit application to an insured bank or to an entity that makes in whole or part, federally related mortgage loans as defined in RESPA of 1974. Such statements or reports must have been capable of influencing the financial institution’s credit decision. Actual damage or reliance on such information is not an essential element of the offense.

The statute applies to the following:

- Applications,
- Advances,
- Discounts,
- Purchases,
- Purchase agreements,
- Repurchase agreements,
- Commitments,
- Credit renewals,
- Extensions or Deferments.

The statute applies to willful omissions as well as affirmative false statements. Obsolete information in the original loan application is not covered unless the applicant reaffirms the information in connection with a renewal request.

18 U.S.C. § 1028 - Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information

This statute applies to persons who knowingly and without lawful authority produce or transfer an identification document, authentication feature, or a false identification document. This statute also applies to persons who knowingly possess with intent to use or transfer unlawfully five or more identification documents. Further, the statute applies to those who knowingly and unlawfully transfer, possess, or use a means of identification of another person with the intent to commit, or to aid or abet, or in connection with any unlawful activity that constitutes a violation of federal law, or a felony under any applicable

state or local law. Finally, this statute covers trafficking in false or actual authentication features for use in false identification documents.

Identification document is defined as a document made or issued by or under the authority of the U.S. government, state or local government, or by a foreign government.

Means of identification is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including:

- Any name,
- Social security number,
- Date of birth,
- Official state or government issued driver’s license or identification number,
- Alien registration number,
- Government passport number,
- Employer or taxpayer identification number,
- Unique biometric data (fingerprints, voice, retina or iris image),
- Unique electronic identification number, address, or routing code, or
- Telecommunication identifying information or access device.

18 U.S.C. § 1028A - Aggravated Identity Theft

Persons who during and in relation to §1341, §1343, or §1344, knowingly transfer, possess, or use, without lawful authority, a means of identification of another person, will in addition to punishment for the conviction of §1341, §1343, or §1344, will be sentenced to a term of two years.

18 U.S.C. § 1029 - Fraud and Related Activity in Connection with Access Devices

This statute applies to persons who knowingly and with the intent to defraud, produces, uses, or traffics in one or more counterfeit access devices, **or** during any one-year period, obtains anything of value using an unauthorized access device with an aggregate value of \$1,000 or more.

The statute also specifically prohibits whoever knowingly and with intent to defraud:

- Possesses 15 or more devices which are either counterfeit or unauthorized [§1029(a)(3)];
- Produces, traffics in, or has control, custody, or possession of device-making equipment [§1029(a)(4)];
- Effects transactions with 1 or more access devices issued to another person(s) to receive payment or other

value of \$1,000 or more over a 1-year period [§1029(a)(6)] ; or

- Uses, produces, traffics in, has control, custody, or possession of a modified or altered instrument to obtain unauthorized use of telecommunications services, [§1029(a)(7) and (9)] among other factors.

Further, soliciting a person for the purpose of offering an access device, or selling information or an application to obtain an access device is covered, as is causing or arranging for another person to present a credit card for payment evidences or records of transactions made by an access device[§1029(e)(7)] .

The term access device is defined as:

- Any card,
- Plate,
- Code,
- Account number,
- Electronic serial number,
- Mobile identification number,
- Personal identification number,
- Other telecommunications service, equipment, or instrument identifier, or
- Other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than solely by paper instrument).

18 U.S.C. § 1030 - Computer Fraud

This statute applies to persons who knowingly access a computer without authorization [§1030(a)(1)], or exceed authorized access levels; or who, having accessed a computer with authorization [§1030(a)(2)], but use it for unauthorized purposes [§1030(a)(2)(A)] (e.g., obtaining information contained in records of a financial institution or card issuer, or a file of a consumer reporting agency). This statute also applies to trafficking in any password or similar information through which a computer may be accessed without authorization [§1030(a)(6)] if such trafficking affects interstate or foreign commerce or if the computer is used by or for the U.S. government. Further, the statute covers those who have the intent to extort money or other thing of value by transmitting any interstate or foreign communication containing a threat to cause damage to a protected computer; threat to obtain information from a protected computer without authorization, or in excess of authorization, or to impair the confidentiality of information obtained from a protected computer; or, demand or request for money or other thing of value in relation to damage to a protected computer,

where such damage was caused to facilitate the extortion [§1030(a)(7)]. Finally, whoever conspires to commit or attempts to commit an aforementioned offense is also covered by this statute [§1030(b)].

§ 1030(a)(2) applies to the observation or reading of the data and does not require the copying or transporting of the data. In addition, the provision does not require larcenous intent.

Other applicable provisions include the following:

- §1030(a)(4) - Prohibits computer intrusion
- §1030(a)(5) - Concerns damage or destruction of a financial institution's property

18 U.S.C. § 1032 - Concealment of Assets from FDIC

This statute applies to persons who knowingly conceal or endeavor to conceal an asset or property from the FDIC acting as conservator or receiver. This statute also covers impeding the FDIC as conservator or receiver, or placing assets or property beyond the reach of FDIC as conservator or receiver.

18 U.S.C. § 1037 - Fraud and Related Activity in Connection with Electronic Mail also known as the "Can-Spam Act of 2003"

This statute applies to those who, in or affecting interstate or foreign commerce, knowingly access a financial institution's computer without authorization and intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer; use a financial institution's computer to relay or retransmit multiple commercial electronic mail messages with the intent to deceive or mislead recipients, or any internet access service as to the origin of such messages; materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages; register, using information that materially falsify the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiate the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names; or falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of five or more internet protocol addresses and intentionally initiate the transmission of multiple commercial electronic mail messages from such address, or conspires to do so.

Chapter 63 - Mail Fraud and Other Fraud Offenses**18 U.S.C. § 1341 - Frauds and Swindles, also known as the Mail Fraud Statute**

This statute covers the use of the mail by sending or receiving items in furtherance of a fraudulent scheme. Note that the statute applies to items sent or received through the U.S. Postal Service and through “any private or commercial interstate carrier.” In recent years, this statute has been used to prosecute the perpetrators of check kiting, advance fee, and mortgage fraud schemes where checks or other documents were sent or received through U.S. mail or interstate carriers. Use of the mail after a scheme to defraud has been completed is not an offense under this statute. See also §1349 Attempt and Conspiracy.

18 U.S.C. § 1342 - Fictitious Name or Address

This statute covers the use of a false, assumed, or fictitious name, address, or title for the furtherance of a fraudulent scheme or device mentioned in § 1341.

18 U.S.C. § 1343 - Fraud by Wire, Radio, and Television also known as the Wire Fraud Statute

This statute applies to a scheme or an artifice to defraud or to obtain property or money through use of wire, radio, or television transmissions in interstate commerce. Recently, in addition to the prosecution of wire and Automated Clearing House transaction fraud cases, this statute has been used to prosecute cases in which commercial and mortgage loan proceeds were wired between states. This statute is also used to prosecute computer-related crimes. See also §1349 Attempt and Conspiracy.

18 U.S.C. § 1344 - Bank Fraud

The statute covers the use of a scheme or artifice to defraud an insured institution or to obtain, through misrepresentations, any of the monies, funds, credits, assets, securities, or other property owned by, or under the control of, the institution. The intent to defraud must be shown, although the scheme does not have to be successful.

Examples:

- Check kiting.
- Diverting loan proceeds for purposes other than stated, including repayment of other debt.
- Out-of-trust in floor plan lending.

18 U.S.C. § 1349 - Attempt and Conspiracy

Any person who attempts or conspires to commit any offense under this chapter will be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy. The conspiracy part of this statute is used frequently in the indictment of individuals.

Chapter 73 - Obstruction of Justice**18 U.S.C. § 1517 - Obstructing Examination of a Financial Institution**

This statute applies to persons who corruptly obstruct or attempt to obstruct any examination of financial institution by an agency of the United States with jurisdiction to conduct an examination. The FDIC has agreed to report any such offense to the FDIC Office of the Inspector General (OIG).

18 U.S.C. § 1519 - Destruction, Alteration, or Falsification of Records in Federal Investigations and Bankruptcy

This statute applies to any person who knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the U.S. or any case filed under title 11, or, in relation to or contemplation of any such matter or case.

Chapter 83 - Postal Service**18 U.S.C. § 1708 - Theft or Receipt of Stolen Mail**

This statute applies to persons who steal, take, or abstract, or by fraud or deception obtain, or attempt to obtain, from or out of any mail, post office, or station thereof, letter box, mail receptacle, or any mail route or other authorized depository. This statute also covers those who buy, receive or conceal, or unlawfully has in his possession, any item stolen, taken, embezzled, or abstracted.

Chapter 95 - Racketeering**18 U.S.C. § 1952 - Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises**

This statute is being used in a manner similar to that of the Foreign Corrupt Practices Act. See 15 U.S.C. § 78dd on the following page. The “Travel Act” applies to those who travel in interstate or foreign commerce or use the mail or any facility in interstate or foreign commerce with the intent to distribute the proceeds of any unlawful activity or commit any crime of violence to further any unlawful

activity or otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity.

Unlawful activity is defined in the statute as any business enterprise involving gambling, liquor which lacks the federal excise tax, narcotics or controlled substances; or, extortion, bribery, or arson in violation of state laws.

18 U.S.C. § 1956 - Laundering of Monetary Instruments

This statute makes it illegal to conduct or attempt to conduct a financial transaction knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity with the intent to promote the carrying on of specified unlawful activity; with the intent to engage in conduct constituting a violation of § 7201 (attempt to evade or defeat tax) or 7206 (false tax returns) of the Internal Revenue Code or knowing that the transaction is designed in whole or part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the specified unlawful activity or to avoid a state or federal transaction reporting requirement.

The statute also makes it illegal to transport or attempt to transport internationally a monetary instrument or funds with the intent to promote the carrying on of specified unlawful activity or knowing that the monetary instrument or funds constitute the proceeds of some form of illegal activity and knowing that the transportation is designed in whole or part to conceal the nature, location, source, ownership or control of the proceeds, or to avoid a transaction reporting requirement under state or federal law.

18 U.S.C. § 1957 - Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity

This statute makes it illegal to engage or attempt to engage in a monetary transaction in property constituting, or derived from, proceeds obtained from a criminal offense knowing that it is criminally derived property and has a value of over \$10,000.

Chapter 103 - Robbery and Burglary

18 U.S.C. § 2113 - Bank Robbery and Incidental Crimes

In addition to covering theft of bank property by force, violence, or intimidation, this section also covers the entry or attempted entry of a bank building with intent to commit any felony affecting any bank and in violation of any statute of the United States, or any larceny.

Chapter 113 - Stolen Property

18 U.S.C. § 2314 - Transportation of Stolen Goods, Securities, Moneys, Fraudulent State Tax Stamps, or Articles Used in Counterfeiting

This statute applies to persons who transport, transmit, or transfer in interstate or foreign commerce, any goods, wares, merchandise, securities, or money in the amount of \$5,000 or more, knowing that the transferred assets were stolen, converted, or taken by fraud. This statute covers falsely made, forged, altered, or counterfeited securities or tax stamps and the device(s) used to make such securities, tax stamps, or traveler checks bearing a forged countersignature. This section does not apply to falsely made, forged, altered, counterfeited obligation or security issued by the U.S. government, or that of any foreign government. This statute may be used in the prosecution of reverse mortgage fraud schemes.

18 U.S.C. § 2315 - Sale or Receipt of Stolen Goods, Securities, Moneys, of Fraudulent State Tax Stamps

This statute prohibits receipt, possession, concealment, storage, bartering selling, or disposing of goods, wares, securities, moneys in the amount of \$5,000 or more, or pledges or accepts as security for a loan any collateral of \$500 or more, which have crossed state or U.S. borders after being stolen, unlawfully converted, or taken, knowing the same to have occurred.

18 U.S.C. Title 15 - Commerce and Trade Chapter 2B - Securities Exchanges

15 U.S.C. §§ 78dd and 78ff - Foreign Corrupt Practices Act (FCPA) of 1977

The FCPA is actually part of the Securities Exchange Act of 1934 and has two main provisions: the anti-bribery provisions; and the books, records, and internal control provisions. The anti-bribery provisions of §78dd-1 are applicable to issuers; §78dd-2 is applicable to domestic concerns, which are defined as a U.S. resident or citizen or any entity such as a partnership or corporation having its principal place of business in the U.S. and being organized under state (or comparable, such as territory) laws; and §78dd-3 is applicable to persons other than issuers or domestic concerns. § 78ff covers the penalties associated with violations of §78dd.

In general, the provisions make it unlawful for any person or entity to corruptly use the mail or other means of interstate commerce to further an offer, payment, or promise to pay any money, offer, or gift, etc., to any foreign official in violation of the lawful duty of such

official in order to assist the issuer in obtaining or retaining business. See also, 18 U.S. C. 1952 Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises

31 U.S.C. Chapter 53

- Subchapter II - Monetary Transactions
- Subchapter III - Money Laundering

Refer to the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual for discussion.

42 U.S.C., Chapter 8A, Subchapter III, § 1490s - Enforcement Provisions, (a) Equity Skimming

Whoever, as an owner, agent, employee, or manager, or is otherwise in custody, control, or possession of property that is security for a loan made or guaranteed, willfully uses, or authorizes the use, of any part of the rents, assets, proceeds, income, or other funds derived from such property, for any purpose other than to meet actual, reasonable, and necessary expenses of the property shall be fined or imprisoned.

←

SIGNIFICANT CIVIL STATUTES

Title 31 - Money and Finance

31 U.S.C. §3729-3733 False Claims Act (FCA)

This civil statute allows for triple damages for the amount that the government paid for false claims submitted. This statute covers many areas unrelated to financial institutions; however, it is currently being used against those who misrepresented the terms and quality of the loans insured by FHA. The statute was amended by the Fraud Enforcement and Recovery Act of 2009, the Dodd-Frank Act, and other acts. FCA lawsuits may be brought by individuals working for financial institutions who file claims on behalf of the government; the U.S. government may or may not join such lawsuits. As a civil action, either the individual or the U.S. government must prove each false claim to the standard of preponderance of evidence. The FCA has a 10-year statute of limitations.

The following are the four major liability clauses within §3729:

- §3729(a)(1)(A) Any person who knowingly presents or causes to be presented, a false or fraudulent claim for payment or approval by or to the U.S. government.
- §3729(a)(1)(B) Any person who knowingly makes, uses, or causes to be made or used, a false record or

statement material to get a false or fraudulent claim paid or approved by the U. S. government. Both this provision and §3729(a)(1)(A) are required to pursue claims under the Act.

- §3729(a)(1)(C) involves conspiracy to commit a violation of §§3729(a)(1)(A) - (G). The conspiracy applies in getting a false claim paid as in §3729(a)(1)(A) or conspiring to underpay the government as in §3729(a)(1)(G).
- §3729(a)(1)(G) Any person who knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government is liable under the FCA.

Under the FERA amendment, material is now defined as having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.

Other sections:

§3730 - Civil Actions for False Claims

§3731 - False Claims Procedures

§3732 - False Claims Jurisdictions

§3730 - Civil Investigative Demands