VI. SOURCES OF INFORMATION

In most fraud examinations, a fraud examiner must obtain documentary evidence from both internal and external sources. In any internal investigation, a large proportion of the documentary evidence that is gathered will come from inside the company. It should be remembered, however, that public and non-public records can also help provide information necessary to conduct a successful fraud examination.

This chapter covers a variety of public and non-public information resources available to the fraud examiner. Some—principally those maintained by agencies—are available simply for the asking. Others are restricted to law enforcement agencies, while still others can be accessed only by means of court proceedings such as subpoenas. This chapter also includes references to directories and databases which can be accessed with little or no cost to find information on virtually anyone.

The fraud examiner must be certain that information obtained is done so legally. Records from confidential sources generally cannot be introduced as evidence. In criminal cases, illegally obtained documentary evidence falls under the exclusionary rule. In civil cases, using illegally obtained documentation might give rise to tort actions or other sanctions against the fraud examiner.

A vast array of information sources are available to the fraud examiner to assist in:

- Locating individuals or verifying their identities
- Researching assets or financial positions
- Documenting lifestyles and background information
- Discovering banking/creditor relationships
- Identifying business affiliations/associates
- Uncovering litigation history.

In-House Sources

A fraud examiner can learn a great deal about an individual by examining routine in-house information on file at the subject's place of business. Reviewing internal sources can provide the framework necessary for continued investigation from other sources. In-house sources include:

- Personnel files
- Other company records
- Prior audit and investigative files
- Disclosure statements
Sources of Information

Personnel Files
Personnel files contain a wealth of information that can be useful in an asset investigation. Usually included in personnel files are the employment application, personnel reviews, salary history, records of disciplinary action, inquiries from outside sources requesting information, and other information. In the employment application, the employee's address, telephone number, family members, and a list of previous employers can be found. The salary history of the employee will also be useful in financial analysis. Often the spouse and the spouse's employer will be listed as an emergency contact, and this might prove useful. Inquiries from outside sources, such as calls from loan companies, banks processing loan applications, or notices of garnishment of wages, might reveal the person's financial condition. Personnel reviews are useful and might help develop the behavioral profile of the suspect and give clues as to the personal habits of the employee.

Other Company Records
Other company records that should be reviewed are the employee's deductions on their paycheck as well as the endorsement on their paycheck. The endorsement might indicate bank accounts previously unknown or people associated with the employee who should also be investigated. Some companies receive information concerning insurance paid on behalf of the employee. While specific medical information might not be available to the fraud examiner, learning that the company paid out numerous claims could be a clue that the employee is in need of money or worse collecting on phony insurance claims.

In addition, other company records such as board of directors' minutes, human resource policies, corporate policies, or the like could prove helpful to the fraud examiner. These policies can show the employer's expectations of their employees and what is considered inappropriate behavior, such as accepting gifts from vendors.

Prior Audit and Investigative Files
Prior audit and investigative files are also useful sources of information. If the suspect has been investigated for improper activity, this might give the fraud examiner leads to follow in the current case. The files might show internal and external relationships, prior interviews, known assets, bank accounts, and the results of their investigation.

Disclosure Statements
Many companies require that, on an annual basis, their employees submit disclosure statements listing all potential conflicts of interest or outside interests that could be harmful to the company. Some of the items located in these statements might include investments, businesses, and people that could be beneficial in determining the suspect's financial condition.
The Right to Access Information

When external documents are needed, fraud examiners should consider accessing public records. Public records are defined as records that a government unit is required by law to keep or that is necessary to keep in order to discharge the duties imposed by law.

There is a great deal of information available as a matter of public record. In fact, the government is bound by law to facilitate the public’s access to government information and to encourage a diversity of sources to acquire and use the information. There are three tenets supporting the public’s right to access government records:

- The public has a broad right of access to government information
- The government may not discriminate in the dissemination of public information
- Restrictions on the use of public information are contrary to government policy in general

Despite the public’s broad right of access, there are numerous laws that limit access to certain types of information and a number of risks to privacy are raised by the collection of information. Therefore, fraud examiners must be certain that information obtained is done so legally.

The federal statutes that most directly affect investigators’ rights to access public records are:

- The Freedom of Information Act
- The Fair Credit Reporting Act
- The Gramm-Leach-Bliley Act
- The Telephone Records and Privacy Protection Act
- The Privacy Act of 1974
- The Right to Financial Privacy Act
- The Driver’s Privacy Protection Act
- The Health Insurance Portability and Accountability Act

Freedom of Information Act (FOIA)

The FOIA is the primary act that governs the availability of governmental records to the general public. The Act sets very specific guidelines on which governmental records are open to the public and which are not. The records that are available are known as “public records,” which are raw records of information that are compiled and maintained by government agencies. The various records are maintained at one of the three government levels: federal, state, or county/local. Although the FOIA is a federal Act, most states have adopted very similar versions of the FOIA to cover the state and local jurisdictions. While these versions are similar to the original FOIA, the individually passed state Acts may differ slightly in specific legal areas from state to state.
Sources of Information

The FOIA and its individual state counterparts regulate:

- The type of records that a governmental agency may maintain about a person.
- The conditions under which such information may be disclosed to another government agency.
- The circumstances and methods under which an individual may obtain copies of agency records that pertain to him.

Generally speaking, government records about an individual are prohibited from release. The disclosure of these records constitutes an invasion of privacy. A person may obtain copies of his own records by requesting them in writing from the agency that maintains them. Such requests often are denied, in whole or in part, because of numerous exceptions to the disclosure requirements. Some of these exceptions include the pendency of an ongoing investigation or concerns about national security. A person denied access to records may appeal through that agency or through the courts.

Most records are maintained at the county or local level, a fact which can seriously hamper any fraud investigation; it can be very difficult for the fraud examiner to catch up with a fraudster who understands the county filing procedures and chooses to operate in different counties. However, there are records available at different governmental levels.

The FOIA provides for public access to the following information:

- Tax rolls
- Voter registration
- Assumed names
- Real property records
- Divorce/probate suits

Information NOT deemed to be public records under the FOIA are:

- Banking records
- Trust records
- Telephone records
- Passenger lists
- Stock ownership

**Fair Credit Reporting Act (FCRA)**

One of the primary statutes limiting access to information is the federal Fair Credit Reporting Act (FCRA). This statute regulates the dissemination of consumer information to third parties by consumer reporting agencies. Historically, the FCRA only applied to consumer credit reports; however, due to amendments in 1997, the FCRA now applies to the gathering of many other types of information about
Sources of Information

an individual through third parties. The Act was amended again in 2003 to provide an exception for investigations involving workplace misconduct.

If the FCRA does apply, it means that an examiner cannot obtain certain information about a person unless that person has received certain notices and signed a consent form. The failure to do so can mean civil penalties.

**Consumer Reports**
In order for the FCRA to apply, the information that is being obtained must be a consumer report. A consumer report is defined as any written, oral, or other communication by a consumer-reporting agency bearing on a customer's credit worthiness, credit standing, character, general reputation, personal characteristics or mode of living.

The Federal Trade Commission (FTC), which is the federal agency responsible for enforcement of the FCRA, has interpreted this to mean basically any information collected on a person. It does not only refer to credit reports. It would also apply to public records such as criminal records and DMV searches.

**Consumer Reporting Agency**
Notice that the information must be gathered from a consumer-reporting agency (CRA). A CRA is defined as anyone who sells information about people. It could be an online service such as ChoicePoint or LexisNexis, or it could be a private investigator.

**Complying with the FCRA**
Before you can get a consumer report for pre-employment purposes, you must comply with the following. However, if you are gathering the information in connection with a workplace investigation of misconduct, you may be excluded from the FCRA (see the Workplace Investigations of Fraud and Misconduct section below). If the FCRA applies, then you must (1) provide the individual with a “clear and conspicuous” separate written disclosure that the employer might obtain a report, and (2) obtain the individual's written authorization. The disclosure and the authorization can be contained in the same document.

If you rely on a consumer report for an adverse action (e.g., denying a job application, reassigning or terminating an employee, or denying a promotion), then you must provide the individual with a pre-adverse action disclosure before taking the adverse action. This disclosure must include a copy of the individual's consumer report and a copy of “A Summary of Your Rights Under the Fair Credit Reporting Act,” which is available from the FTC.
Sources of Information

After adverse action is taken, you must notify the individual via an adverse action notice that the action has been taken. That notice must include the following:

- Name, address, and phone number of the consumer reporting agency (CRA) that supplied the report
- A statement that the CRA did not make the adverse action decision and cannot explain why the adverse action was taken
- A notice of the individual's right to dispute the accuracy or completeness of the information furnished, and a notice of the individual's right to an additional free consumer report from the agency upon request within 60 days

Investigative Consumer Report

Under the FCRA, as amended, an investigative consumer report is a report containing information about an individual's character, general reputation, personal characteristics, or mode of living that is obtained through personal interviews with neighbors, friends or associates. If such a report is made, then other notices and consents may need to be obtained from the individual. For example, a separate disclosure must be used to inform the employee that an investigative consumer report is being obtained. The form must also state what sort of information will be collected.

In addition, the company must disclose to the individual the nature and scope of the investigation (if he or she requests). If any adverse action is to be taken against the person, he or she can ask to receive a copy of the report before such action is taken. Further, the report given to the individual must not be redacted, meaning that if the report contains names of the people providing the information and what they reported, such information could not be deleted from the report. The person must also be given an opportunity to dispute the findings in the report.

When the FCRA Does Not Apply

The FCRA does not apply if the person or organization seeking the information gathers it directly from the source. For instance, assume you are employed by a company and you are asked to conduct an investigation concerning a possible fraud by another employee. You want to check federal criminal records to see if the suspect has been convicted of any previous crimes. If you or an employee of your company personally goes to the courthouse and looks for the records, then the FCRA does not apply.

However, if you use a third party to gather the information, such as a private investigator or an online public records service, then you must comply with the notice and consent provisions of the FCRA.

Workplace Investigations of Fraud and Misconduct

The Fair and Accurate Credit Transactions Act of 2003 amended the FCRA to exempt certain reports involving employee misconduct investigations.
Sources of Information

As a result of these new amendments, an employer who uses a third party to conduct a workplace investigation no longer has to obtain the prior consent of an employee if the investigation involves suspected:

- Misconduct
- Violation of law or regulations
- Violation of any pre-existing policy of the employer

To qualify for this exception, the report from the third party must not be communicated to anyone other than the employer, an agent of the employer, or the government.

However, if “adverse action” is taken against the employee based on the results of the investigation, the FCRA still requires that the employer to provide the employee with a summary of the report. “Adverse action” is broadly defined as any employment decision that adversely affects the employee. The summary must “contain the nature and substance of the communication upon which the adverse action is based.” However, it does not have to identify the individuals interviewed or the sources of the information.

Contact Your Attorney
Unfortunately, for fraud examiners, the FCRA has created several more hoops that examiners must jump through before they can obtain certain types of information. The FCRA is not clearly written, but the Federal Trade Commission has published several letters giving its interpretation of the statute. These letters and the text of the FCRA can be obtained through their website at www.ftc.gov. Because of the potential pitfalls involved, it is recommended that a consumer credit report should be used only if the information needed cannot be obtained elsewhere.

The most important thing for fraud examiners to remember is to consult your in-house or outside counsel. Your attorney will help you determine what procedures you need to institute to comply with the FCRA.

Gramm-Leach-Bliley Act
The Gramm-Leach-Bliley Act (GLB) was passed in 1999 and final rules implementing the Act became final in 2001. GLB was originally enacted to allow banks and other companies to offer previously forbidden services such as insurance and securities brokerage services. Congress was worried that these new “super banks” would share customers’ financial data to affiliates and other companies to hawk their new products. Therefore, Congress added a provision requiring financial intuitions to tell customers about its privacy policy, to notify them of private information the institution intends to share, and to give customers the chance to block such information sharing.
Sources of Information

To implement the new law, Congress ordered regulators to define financial institution in the broadest possible terms. Thus, financial institutions include not just banks, but also insurance companies, accountants, tax preparation and real estate settlement services, and investment advisors. The text of the rule can be found at 16 C.F.R. Part 313.1. Additional information about the rule can be found at the Federal Trade Commission's website located at www.ftc.gov.

The problem for fraud examiners is that the privacy rules implemented as part of the GLB have been interpreted to prevent the selling of credit header information. Under the FTC's interpretation of the rule, credit header information cannot be sold except for the very limited purposes allowed under the Fair Credit Reporting Act. The agency reached this decision by concluding that such basic personal information, such as names and addresses, is "financial" information, and, therefore, must be protected by under the GLB Act. Unfortunately, this prevents credit bureaus from selling credit header information (including names, addresses, phone numbers, and Social Security numbers) to private investigators, direct marketers, or other information brokers.

The credit bureaus challenged the FTC's rule in court. However, in May 2001, the U.S. District Court for Washington, D.C. upheld the agency's interpretation. The credit bureaus have appealed that decision. Unless the decision is overturned, it appears that it will be more difficult for fraud examiners and investigators to obtain personal information about potential suspects or witnesses.

GLB also made it a criminal offense to engage in "pretexting." Some individuals used pretexting as a means to gather financial information about a subject. Pretexers would contact a financial institution and pretend to be the customer or someone else authorized to obtain financial information and basically trick the financial institution into providing information about the subject.

Section 6821 of Title 15, United States Code, (added by GLB) makes it an offense to:

- Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution
- Ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents

Violators can, under certain circumstances, be fined and/or imprisoned up to 10 years.
Sources of Information

Telephone Records and Privacy Protection Act
The Telephone Records and Privacy Protection Act of 2006 (TRPPA) also criminalizes pretexting. In 2006, pretexting garnered much criticism after Hewlett-Packard admitted that to uncover boardroom leaks, its investigators obtained phone records of journalists and board members through pretexting. Within four months of the scandal's public release, President Bush signed the TRPPA into law.

Specifically, the TRPPA criminalizes the practice of obtaining and attempting to obtain, sell, or buy confidential phone records through the use of false statements, unless otherwise permitted by law. Violations of the Act are criminal and if convicted, a violator faces up to 10 years in prison and up to $100,000 in fines. These fines and prison terms may be increased in case of violation compounded with other activities, or some egregious crimes.

Before engaging in any type of pretexting activity, investigators should consult with an attorney to determine whether the information sought is protected by state or federal law as well as whether the planned impersonation method is legally acceptable.

Privacy Act of 1974
The Privacy Act of 1974 restricts information about individuals, both employees and non-employees, that might be gathered by government agencies. An agency might maintain records about a person containing information that is relevant and necessary to accomplish a purpose of the agency. This information might include a person's education, finances, medical history, criminal history, employment history, and identifying information (fingerprint, voiceprint, or photograph). The employee might have access to the information unless it is investigatory material compiled for law enforcement purposes, statistical records, or material compiled solely for determining suitability, eligibility, or qualification for federal service or promotion.

Right to Financial Privacy Act
The Right to Financial Privacy Act prohibits financial institutions from disclosing financial information about individual customers to government agencies without:

- The customer's consent
- A court order
- Subpoena
- Search warrant
- Other formal demand, with limited exceptions

Although the statute applies only to demands by government agencies, most banks and other financial institutions also will not release such information to private parties absent legal process, such as a subpoena issued in a civil lawsuit.
Sources of Information

**Driver’s Privacy Protection Act**
The Driver’s Privacy Protection Act bars states from releasing drivers’ Social Security numbers, photographs, or certain other information unless they obtain “the express consent” of the person in advance.

This Act makes it extremely difficult to obtain almost any up-to-date information from state motor vehicle departments because such information can only be obtained if the driver has expressly consented to its release. Therefore, companies may wish to consider having employees sign a consent form as early as the employment application stage.

**Health Insurance Portability and Accountability Act**
The Health Insurance Portability and Accountability Act (HIPAA) instituted several new privacy rules. While most of the rules do not directly affect investigations, fraud examiners should be aware of the rules because they may have an impact on the type of information that can be legally gathered on employees.

The HIPAA privacy rules place restrictions on the availability and use of “protected health information.” The definition of this term is extremely broad and covers any information relating to an individual’s past, present, or future physical or mental health, payment for services, or health care operations. For example, a cancer center employee, who stole a patient’s identification information to obtain credit cards, pled guilty to violating HIPAA. This case marked a significant point in HIPAA legislation because it had so little to do with actual health information, and more to do with identity theft, but was covered under the statute.

If information about the health of an individual, or payments for services, becomes an issue during an investigation, you should immediately contact the human resources (HR) department. The HR department should have information about whether the entity is subject to the HIPAA rules and can assist you in compliance with those rules.

The most important thing to note is that if the HIPAA rules apply, you are restricted as to the type of health information you can access without specific written authorization. You should never contact the health care provider, the health plan administrator, or a medical billing services for copies of employee records without first consulting the employer’s legal counsel or the HR department.
Sources of Public Information

Much information regarding an individual's personal and business history is a matter of public record; therefore, fraud examiners must determine those points of identity that give the subject individualism and separate that person from others with the same name or set of circumstances.

Many types of public records contain similar information about individuals or entities. Yet, other agencies or governmental units are responsible for specific functions that require them to maintain unique information. An examiner should be prepared to consult a variety of public records to gather the necessary information.

Public information can be useful for a number of reasons. It can supply invaluable background information on employees, suspects, and witnesses. It can be used to corroborate or refute witness statements, it can help investigators track the flow of stolen cash or other assets, and it can be extremely important in a company's efforts to recover losses.

The following sections describe several public record sources that examiners can easily access at the city, county, state, and federal levels of government.

City Government

Building Inspector

The following information generally is available through the office of a city's building inspector:

- Building permits, showing the name of applicant, address of construction, estimated cost, and the name of the builder or contractor
- Blueprints and plans showing construction details that often are submitted with applications for building permits
- Building inspectors' reports, containing information regarding compliance with construction specifications

Health Department

Most county health or fire departments conduct routine inspections of businesses for health and safety code or fire code violations. These inspectors may have valuable information about the business, including its operations, employees, and owners.

Death certificates usually can be found at city, county, or state health departments. A death certificate provides the name of the deceased, address, sex, age, race, birthplace, birth date, death place, date and time of death, Social Security number, medical certificate, and coroner's certificate. Additionally, a death certificate generally provides information about the deceased's parents and their occupations.