

Leading With Integrity

The Equifax Business Ethics and Compliance Program

Table of Contents

Introduction

I. About the Equifax Business Ethics and Compliance Program	3
II. Program Administration and Sanctions	3
III. Employee Reporting Procedures and Investigating Misconduct	4
▪ What to Report.....	4
▪ How to Report Misconduct.....	4
▪ How to Contact the Compliance Officer.....	5
▪ How to Report Suspected Accounting or Auditing Misconduct.....	5
▪ You May Remain Anonymous or Request Confidentiality.....	6
▪ Investigations Are Confidential.....	6
▪ You May Not Be Treated Unfairly Because You Have Reported a Suspected Violation.....	6
▪ Improper Uses of Reporting.....	6
Core Business Ethics and The Equifax Way	7
I. Core Business Ethics	7
II. The Equifax Way.....	7
Code of Conduct.....	7
▪ Introduction.....	8
I. Human Resources	8
▪ Policy Against Harassment.....	7
II. Substance Abuse.....	10
III. Political Participation	10
IV. Environment, Health and Safety	10
V. Accounting Integrity and Internal Controls.....	11
▪ Senior Financial Officers.....	11
▪ Internal Control and Control Activities	11
▪ Accounting Standards	12
▪ Cash Disbursements	12
▪ Cash and Check Acceptance.....	12
▪ Full Disclosure Requirements	12
▪ Reporting of Irregularities	13
VI. Fraud and Embezzlement	13
VII. Regulatory Requirements In Our Core Business	13
▪ Fair Credit Reporting Act.....	13
▪ Gramm-Leach-Bliley Act.....	14
VIII. The Foreign Corrupt Practices Act.....	15
IX. Conflicts of Interest	16
X. Relationships With Suppliers/Contractors/Customers	17
▪ Special Requirements for Government Contracts.....	17
XI. Records Retention/Destruction.....	18
▪ Litigation Exception.....	18
XII. Antitrust and Trade Regulation	18
XIII. Insider Information and Securities Trading	19
▪ Material Information That is not Public Must be Kept Confidential and not Used.....	19
▪ Material Nonpublic Information Defined.....	20
▪ Insider Trading Defined	20
▪ Insider Training Us a Serious Crime.....	20
▪ Guidelines Compliance	21
XIV. Media Relations	21
XV. Advertising and Statements to Customers.....	21
XVI. Confidential Information and Intellectual Property	21
▪ Confidential Information.....	21
▪ Intellectual Property.....	22
▪ Rights of Others.....	23



Introduction

I. About the Equifax Business Ethics and Compliance

Our Collective objective as Equifax officers and employees is to maximize the value of our shareholders' investment in the Company, while conducting our business in a manner that is socially responsible, value-based, and in compliance with the letter and spirit of the law. Therefore, we have developed this booklet, "Leading with Integrity," as part of our Business Ethics and Compliance Program.

The Program includes two main components: (1) this Business Ethics and Compliance Manual, which includes a statement of our Core Business Ethics and Code of Conduct (collectively, the "Code"); and (2) Procedures for Program Administration. All officers and employees, as a condition of employment or continued employment, will acknowledge in writing that they have received copies of this Manual, read it, and understand that the Code contains the Company's expectations regarding employee conduct.

You should know that the Program is designed to satisfy the standards contained in the Federal Sentencing Guidelines published by the U.S. Department of Justice. U.S. federal courts are bound to apply those Guidelines when sentencing companies convicted of federal offenses arising from the illegal acts of one or more employees. Those Guidelines provide for substantial leniency in sentencing of the company from otherwise severe mandatory penalties, where the company had in effect an adequate compliance program at the time of the illegal activity.

In general, the Company intends to cooperate in connection with any government investigation of alleged criminal conduct, and will coordinate all activity in connection with those investigations through the Company's General Counsel.

Equifax anticipates that any waivers of provisions of the Code will be infrequent and granted only when justified by unusual circumstances not contemplated by the Program. Any waiver of any part of the Code for executive officers may be made only by the Board of Directors or an authorized Board committee. Waivers for the benefit of an executive officer shall be publicly disclosed to the extent required by applicable laws or stock exchange listing standards.

II. Program Administration and Sanctions

The Company's General Counsel has responsibility for the Program. The Company has appointed a Compliance Officer who will perform various ongoing administrative functions in connection with the Program, including issuing Code updates and maintaining an anonymous reporting hotline (the Equifax Reporting Line) for receipt of questions and reports of potential employee violations of the Code. As provided in the Program administrative guidelines, the Compliance Officer or another appropriate individual appointed by the General Counsel will investigate all reported violations of the Code so the Company can take appropriate steps to remedy any violation in a prompt manner.

An employee who has violated the Code or otherwise committed misconduct is accountable for his or her violation. Violators may be subject to a full range of penalties of varying levels or severity. These penalties may include, without limitation, oral or written censure, training or re-training, demotion or re-assignment, suspension with or without pay or benefits or termination of



employment. In determining the appropriate penalty for a violation, Equifax may take into account

all relevant information, including the nature and severity of the violation, whether the violation involved fraud or falsehood, whether the violation was intentional or inadvertent, whether the violator cooperated with the investigation of the violation and whether the violator has committed other violations in the past.

III. Employee Reporting Procedures and Investigating Misconduct

▪ What to Report

Our Code is designed to encourage participation by our employees and to provide a method to report conduct that they suspect is in violation of the Code, including applicable laws and regulations.

All employees should be alert and sensitive to situations that could result in misconduct. **If an employee believes that actions have taken place, may be taking place, or may be about to take place that violate or would violate the Code, including applicable laws or regulations, he/she is obligated to bring the matter to the attention of the Company.**

▪ How to Report Misconduct

If you think that certain activity is in violation of the Code, you should generally first bring the matter to the attention of your supervisor. However, if the conduct in question involves your supervisor, if you have reported it to your supervisor and do not believe he/she has dealt with it properly, or if you otherwise do not feel that you can discuss the matter with your supervisor, you may either raise the matter with the next level of management, the Human Resources Department, or report it to the Code of Conduct Compliance Officer.

In reviewing a complaint received from an employee, a supervisor or manager should consider whether the report involves a potential violation of the Code and if so, he/she must report it immediately to an appropriate person. If it involves accounting, internal accounting controls, or auditing irregularities the supervisor must immediately forward the complaint to the General Counsel.

In the event that you have a complaint involving accounting, internal accounting controls, or auditing irregularities, you may alternatively report the matter directly to the General Counsel, as explained below.

The person receiving your complaint or report will respond to it appropriately, and in accordance with any applicable procedures for Program administration or Company policies.



- **How to Contact the Compliance Officer Compliance Officer.**

An employee may communicate with the Code of Conduct Compliance Officer, either anonymously or by name, by any of the following methods:

In writing, addressed to the Code of Conduct Compliance Officer, either by internal mail to:

Mail Drop

H-53 or by U.S. mail to Equifax, 1550 Peachtree Street, NW, Atlanta, GA 30309

- **By e-mail** to “Code of Conduct Compliance Officer” or by Internet at codeofconduct.office@equifax.com do not use e-mail if you wish to report on an anonymous basis)
- **By phoning** the Equifax Reporting Line: (877) 482-5252. For international locations, please refer to Equifax Central (Ethics section) for your access code when dialing.

Employees may also contact the Code of Conduct Compliance Officer by any of these methods with questions about the Program or the Code.

- **How to Report Suspected Accounting or Auditing Misconduct.**

If any employee has a complaint or report involving accounting, internal accounting controls or auditing matters, the employee may report the matter, either by name or on an anonymous basis, to the General Counsel instead of using the complaint procedures outlined above.

If you wish to report questionable accounting or auditing matters to the General Counsel on an anonymous basis, send a written letter addressed to the General Counsel via internal mail to Mail Drop H-63 or by U.S. mail to the address listed in the previous section, or phone the Equifax Reporting Line at (877) 482-5252. Do not e-mail the General Counsel if you wish to report on an anonymous basis.

A questionable accounting or auditing matter could include any of the following:

- Fraud or material misstatements or omissions in financial statements or accounting records.
- Fraud or material involving noncompliance with internal accounting controls.
- Reportable conditions, significant deficiencies or material weaknesses in internal accounting controls.
- Material misconduct in the internal or external auditing process, including improper influence on the conduct of audits.

- **You May Remain Anonymous or Request Confidentiality.**

When reporting conduct suspected of violating the Code, including applicable laws



and regulations, to the Code of Conduct Compliance Officer or reporting questionable accounting, internal control or auditing matters to the General Counsel, you may either remain anonymous or identify yourself. If you wish to remain anonymous, we ask that you provide enough detailed information so that we may thoroughly investigate your complaint and take appropriate action to remedy any Code violations. Do not e-mail the Compliance Officer or General Counsel if you wish to remain anonymous.

If you identify yourself, you may still request that your name be kept confidential. Equifax will use reasonable efforts to keep your identity confidential. You should be aware, however, that Equifax's obligation to investigate the reported matter and take any remedial action may require that your identity be revealed, or the nature of the investigation may be such as to cause your identity to become known.

- **Investigations Are Confidential.**

The Company will also use reasonable efforts to protect the identity of employees about or against whom an allegation is brought unless and until it is determined that a violation has occurred. Any employee involved in any capacity in an investigation of a possible violation of the Code must not discuss or disclose any information to anyone outside of the investigation unless required by law or when seeking his or her own legal advice if necessary.

- **You May Not Be Treated Unfairly Because You Have Reported a Suspected Violation.**

Equifax expressly forbids any retaliation against any employee (or his or her relative or associate employed by Equifax) for making a required or voluntary lawful report of possible misconduct or violation of law that has occurred, is ongoing, or is about to occur. Any employee who participates in any such retaliation is subject to disciplinary action, including termination.

Moreover, it is Equifax's policy not to discharge, demote, suspend, threaten, harass or otherwise discriminate in the terms and conditions of employment against any employee (or his or her relative or associate employed by Equifax) who has reported or otherwise assists in an investigation or proceeding regarding any conduct which the employee reasonably believes relates to a violation of applicable laws or regulations, the Code, or any Equifax policy, by the Company, its officers, employees or agents.

- **Improper Uses of Reporting.**

Employees must not use the Program in bad faith or in a false or frivolous manner. Further, you should not use the Equifax Reporting Line to report personal grievances not involving the Code. You should follow the Company's "Open Door" policy to address those matters.



Core Business Ethics and the Equifax Way

I. Core Business Ethics

Our collective mission is to maximize the value of our shareholders' investment in the Company while maintaining our core business ethics, which are embodied under the following principles:

- We conduct our business in a socially responsible manner within the letter and spirit of both the law and our Code of Conduct;
- We recognize that people are our greatest strength. The quality of our people differentiates us and personifies our leadership position;
- We treat customers, consumers and employees with respect and dignity;
- We are committed to a well-established set of principles that address consumer privacy issues, and we take pride in being a trusted steward of consumer information;
- We take very seriously our reputation for honest and ethical business dealings around the world, and we require our employees to conduct themselves in an honest and ethical manner at all times; and
- We seek customers and business partners whose ethical standards mirror our own, and decline to do business with unethical entities and individuals.

II. The Equifax Way

THE EQUIFAX WAY is a concise statement of how we carry on our business, how we achieve our objectives, and how we maintain a high degree of integrity while succeeding:

The Equifax Way

OPERATING PRINCIPLES

It is all about **growth, innovation**, deployment of **technology**, led by the greatest **people** anywhere.

OUR BUSINESS VALUES

At Equifax we lead with **integrity**, work as a **team**, **respect** all people and are **performance** driven to achieve excellence in all that we do.

Code of Conduct

• Introduction.

This Code of Conduct includes a series of numbered Policy Statements. Some of them are summaries of more complete Company policies. Ultimately, we intend to make available copies of those more complete policies and other supporting information, such as copies of certain pertinent laws and regulations, in an Equifax Compliance Library maintained by the Code of Conduct Compliance Officer on a Company intranet system. Until then, you may obtain complete policies and other available supporting information relating to the Code of Conduct and Compliance Program in the Equifax Code of Conduct Compliance Library by



contacting the Compliance Officer. From time to time, we may publish revisions or supplements to the Policy Statements as appropriate based on changes in the regulatory environment, changes in the business we conduct, or other factors.

The following are the Policy Statements contained in our Code of Conduct. Employees who violate the Code or its underlying policies are subject to disciplinary action, up to and including termination of employment. Specific examples of legal fines or penalties are included with some of the Policy Statements for illustration purposes only. Those examples are not exclusive, and are not intended to be a full description of all possible legal fines or penalties.

All legal obligations constitute an integral and key part of our Code. You are required at all times to comply not only with the specific Policy Statements in this Code, including all laws and regulations discussed below, but also with all other applicable laws and regulations in connection with your employment or service with Equifax. If an express provision of the Code conflicts with a legal obligation, you must follow the law. Contact your supervisor or the Compliance Officer in the event you suspect such a conflict.

I. Human Resources

As reflected by our operating principles, the Company recognizes that its greatest strength lies in the talent and the ability of its employees. The Company's ongoing policy is to protect and nurture this asset.

Equifax is committed to providing equal opportunity in all of our employment practices, including selection, hiring, promotion, transfer, and compensation, to all qualified applicants and employees without regard to race, color, religion, age, sex/gender (including pregnancy, childbirth and related medical conditions), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law. Equifax also practices Affirmative Action, which is the initiation of good-faith efforts to attract, employ, and advance women and minorities, covered veterans, and persons with disabilities so that a mix of qualified candidates is available when employment and promotion decisions are made. We must comply with these policies in every respect, both in letter and in spirit.

- **Policy Against Harassment.**

Equifax does not tolerate harassment of any of our employees, applicants, vendors or customers, and our policy is to maintain a working environment free from harassment. Any form of harassment related to an individual's race, color, religion, age, sex/gender (including pregnancy, childbirth and related medical conditions), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law is a violation of this policy and will be treated as a disciplinary matter.



Harassment is unwelcome conduct toward an individual because of his or her race, color, religion, age, sex/gender (including pregnancy, childbirth and related medical conditions), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law, when the conduct has the purpose or effect of unreasonably interfering with the individual's work performance or creating an intimidating, hostile, or offensive working environment.

For purposes of this policy, sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature, when: submission to such conduct is made either implicitly or explicitly a term or condition of employment; submission to, or rejection of, such conduct by an individual is used as the basis for employment decisions affecting such individual; or such conduct has the purpose or effect of unreasonably interfering with the individual's work performance or creating an intimidating, hostile, or offensive working environment.

Examples of prohibited conduct under this policy include:

- Offensive remarks, negative stereotyping, comments, jokes or slurs, or other verbal or non-verbal conduct, pertaining to or showing hostility or intimidation toward a person because of his or her race, color, religion, age, sex/gender (including pregnancy, childbirth and related medical conditions), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law;
- Offensive sexual remarks, sexual advances, flirtations, propositions, requests for sexual favors or other verbal or nonverbal conduct of a sexual nature regardless of the gender of the individuals involved;
- Unwelcome or offensive physical conduct, including touching, regardless of the gender of the individuals involved;
- Display of offensive or derogatory pictures, drawings or photographs or other communications, including e-mail; and
- Threatening reprisals for an employee's refusal to respond favorably to sexual advances, requests for sexual favors or for reporting a violation of this policy.

Harassment by non-employees of our employees in connection with their work is a violation of this policy. Harassment by our employees of applicants for employment, or employees of our vendors or customers, is also a violation of this policy.

If you believe that you are being harassed, if you believe that someone else is being harassed or if you believe you have been retaliated against for complaining of harassment, you should promptly report it without fear of reprisal if the report was made in good faith. You have several options for making a report:

- Talk to your manager.
- If the problem involves your manager, if you do not want to discuss the problem with your manager, or if you have previously discussed the problem with your manager and believe further action is necessary to resolve the problem, contact your Human Resources Business Partner.
- Call the Ethics and Compliance Hotline toll free @ 1-877-482-5252, 24 hours a day/ 7 days a week. You may remain anonymous in making a complaint via the hotline.



- Contact The Equifax Code of Conduct Compliance Officer by mail: Code of Conduct Compliance Officer, Mail Drop H-53, 1550 Peachtree Street, Atlanta, GA 30309 or by email: codeofconduct.office@equifax.com .

Any supervisor who observes or receives a report of harassment **must** immediately report it to Human Resources or to the Code of Conduct Compliance Officer, no matter how insignificant it may seem to the employee or supervisor.

Human Resources, or its designated representative, will carefully investigate each harassment complaint received by them or the Code of Conduct Compliance Officer and take corrective action when appropriate. The Company will keep your complaint as confidential as reasonably possible and will not penalize you in any way for reporting conduct that you believe in good faith may be a violation of this policy. Retaliation against individuals who in good faith report harassment or discrimination or who assist in an investigation of alleged harassment or discrimination is expressly prohibited.

Violations of this policy will subject an employee to disciplinary action, up to and including immediate termination. Therefore, if you have a question about what constitutes harassing behavior or what conduct is prohibited by this, please discuss it with your supervisor, the Human Resources Department or the Code of Conduct Compliance Officer.

Equifax cannot resolve a harassment problem unless we know about it. Therefore, it is your responsibility to bring any such problems to our attention so that we can take whatever steps are appropriate to correct the problem.

II. Substance Abuse

Equifax does not tolerate being under the influence of or using alcohol in the workplace, the illegal use of drugs, or the abuse of other legally controlled substances. Unlawful actions that discredit the Company involving illegal drugs, controlled substances or alcohol during either working or non-working hours are grounds for disciplinary action, including termination. In order to better ensure a drug-free working environment for the safety and well being of all our employees, Equifax has adopted a Drug and Alcohol Policy, including certain drug screening procedures, a copy of which is in the Company's Employee Handbook and the Compliance Library.

III. Political Participation

U.S. federal and state laws limit the nature and extent of individual and corporate political participation. For example, federal law and that of many states prohibit corporate contributions to political candidates or officeholders.

Federal law and Company policy also states that the Company will not reimburse anyone for personal political contributions. The Company will not alter personal compensation in any way under any circumstances to reflect personal political contributions.

IV. Environment, Health and Safety

The Company is committed to protecting and maintaining the quality of the environment and to promoting the health and safety of employees, customers and the communities where it operates. To meet that commitment employees must:

- Operate in full compliance with both the letter and the spirit of environmental, health and safety laws and regulations;
- Immediately report any environmental, health or safety problems to their manager;
- Consider opportunities to improve environmental, health and safety programs; and
- Be prepared to observe emergency preparedness plans if necessary.

You should directly report any actual or potential environmental, health or safety problems or any questions about employees' responsibilities or Company policies in these areas to your supervisor or the Code of Conduct Compliance Officer.

V. Accounting Integrity and Internal Controls

- **Senior Financial Officers.**

The Chief Executive Officer, the Chief Financial Officer and the Principal Accounting Officer or Controller or persons performing similar functions (referred to collectively as the Senior Financial Officers) are responsible, within the scope of their duties, for promoting full, fair, accurate, timely and understandable disclosure in Equifax's periodic SEC reports and other public disclosures, consistent with applicable laws, rules and regulations. The Code – including the provisions related to honest and ethical conduct, conflict of interest, compliance with law and the obligation to report misconduct or Code violations – is applicable to the Senior Financial Officers to the same extent it is applicable to all other officers and employees. Conduct by any Senior Financial Officer that you suspect violates the Code must be reported to the General Counsel or Code of Conduct Compliance Officer in the manner described earlier in this Code. Only the Board of Directors or an authorized Board Committee may waive application of any part of the Code to any Senior Financial Officer.

- **Internal Controls and Control Activities.**

The Company has established internal controls to provide reasonable assurance of achieving the following objectives:

- Effectiveness and efficiency of operations;
- The safeguarding and proper management of the Company's assets;
- Accurate and timely financial reporting in accordance with generally accepted accounting principles and applicable laws and regulations; and
- Compliance with applicable laws and regulations.

Equifax employees and officers are responsible for complying with internal controls applicable to their areas of responsibility. Also, employees need to be alert to situations, whether in their direct area of responsibility or otherwise, where internal controls could be improved. You may provide any suggestions you have for improving the Company's controls to your supervisor or to the Corporate Controller. No officer, employee or other person acting on behalf of the Company will engage in any activity that circumvents or compromises the Company's systems of internal controls.



A primary purpose of internal controls, including the control activities and cash disbursement and cash and check acceptance policies described below, is to help ensure the protection and efficient use of Equifax's assets. **All Company assets should be used only for legitimate business purposes.**

To achieve its internal control objectives, the Company has implemented certain control activities relating to both manual and automated systems. Examples of control activities include: approvals and authorizations of transactions, segregation of duties, verification of supporting documents, reconciliation of accounts, reviews of key financial reports and operating statistics, physical and logical security of Company assets, and validity checks and balancing procedures for data processing.

- **Account Standards.**

All accounting records and financial statements should be recorded in accordance with U.S. generally accepted accounting principles (GAAP), or that of another jurisdiction where appropriate. In order to provide guidance on GAAP, Equifax Corporate Accounting has established the Equifax Accounting Standards, which is available from Corporate. You should direct questions on the treatment of a particular accounting issue to your supervisor or to the Corporate Controller.

- **Cash Disbursements.**

Company policy prohibits cash disbursements except for nominal disbursements drawn from established and properly recorded petty cash accounts. All checks will be drawn only to the ultimate payee. No checks will be drawn to cash or bearer. You can obtain specific guidance on disbursement procedures from your supervisor or from Corporate Accounting.

- **Cash and Check Acceptance.**

No employee other than those specifically authorized may accept cash or checks or similar negotiable instruments from a customer or vendor unless a manager is present. You must always provide a written receipt to the person providing the payment. The Company may hold any employee who fails to follow this procedure liable for any monetary loss.

- **Full Disclosure Requirements.**

Federal law requires publicly traded companies to provide full, fair, accurate, timely and understandable disclosure in all reports and other documents submitted to the Securities and Exchange Commission (SEC) or in any public communication. Equifax's SEC reports and other public disclosures must be free of material misstatements and misleading omissions. Equifax's public financial information should fairly present in all material respects the Company's financial condition, results of operations and cash flows.



Equifax ensures that such public disclosures are accurate, timely and understandable by maintaining internal accounting controls and internal disclosure controls and procedures (to ensure that information required to be disclosed is accumulated and made known to the appropriate persons in a timely fashion), coordinating all disclosure, and limiting its authorized spokespersons.

- **Reporting of Irregularities.**

If you suspect that any Equifax SEC report, press release or other public disclosure (including on Equifax's website) contains a material inaccuracy or omits material fact that renders the disclosure misleading, you should immediately contact your supervisor, the Corporate Controller or Code of Conduct Compliance Officer, or if it involves a questionable accounting or auditing matter, the General Counsel. You may contact the General Counsel or Code of Conduct Compliance Officer anonymously, as explained above.

VI. Fraud and Embezzlement

According to the American Institute of Certified Public Accountants, fraud and embezzlement includes the following:

- Misappropriation or embezzlement of any Equifax's property, assets or services;
- Intentional misstatements, misclassification or omission in Equifax's financial statements, including intentional misapplication of accounting principles; and
- Manipulation, falsification or alteration of accounting records or supporting documentation.

If you suspect that fraud or embezzlement has occurred, you must immediately notify the Code of Conduct Compliance Officer so that he or she may take appropriate action. **Any type of fraud or embezzlement will result in serious consequences and disciplinary action, up to and including immediate discharge.**

VII. Regulatory Requirements of Our Core Businesses

Although we cannot list all the regulatory requirements that apply to Equifax's operating units around the world, it is appropriate to highlight the following major U.S. laws. Additional information and guidelines pertaining to other applicable laws and regulations in your geographic territory are available in the Equifax Compliance Library.

- **Fair Credit Reporting Act.**

The Federal Credit Reporting Act (FCRA) became effective in 1971 and was materially amended in 1996 and 2003. Its purpose is to ensure that consumer reporting agencies adopt reasonable procedures for meeting that needs of commerce for consumer credit, personnel, insurance, and other information in a manner that is fair and equitable to the consumer with regard to the confidentiality, accuracy, relevance and proper use of that information. The FCRA also regulates the activities of users of consumer reports and furnishers of information to consumer reporting agencies.



The FCRA also seeks to prevent an undue invasion of the right to privacy in the collection and dissemination of consumer reports by limiting the purposes for which reports may be used. The FCRA places disclosure obligations on consumer reporting agencies, as well as on users of consumer reports who reject or otherwise take adverse action on a consumer's application for credit, insurance, employment or other benefits based on the information contained in a consumer report.

In addition to civil liability, the law provides for the imposition of criminal penalties against:

- (1) Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information, or
- (2) Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses.

The penalty may include a fine or imprisonment for not more than two years, or both. We

are a party to a Consent Order with the Federal Trade Commission requiring our U.S. credit reporting business to maintain certain procedures to facilitate FCRA Compliance. Also, various states have laws imposing obligations similar or in addition to the FCRA. The full text of the FCRA as well as similar state regulations and the FTC Consent Order are available in the Equifax Compliance Library.

The Company provides FCRA training courses for employees engaged within this business. You may contact your manager regarding FCRA training opportunities.

▪ **Gramm-Leach-Bliley Act.**

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, sets forth the requirements of financial institutions regarding the privacy and safeguarding of consumers and customers' non- public personal information. Financial institutions must provide consumers and customer's notices regarding the institution's information collection and sharing practices. Along with this notice, consumers and customers must also be given the right to "opt-out" to prevent the financial institution from sharing their information with third parties. Additionally, financial institutions must develop and maintain an information security program to protect the security, confidentiality and integrity of the information. Criminal and civil penalties may be imposed from violations of the Act.

The Gramm-Leach-Bliley Act governs the manner in which various Equifax entities collect, use and disclose consumer and customer information received from financial institutions. Additionally, Equifax entities that receive and collect consumer and customer information have developed and maintain appropriate information security programs.

Equifax provides GLB training courses for those employees employed within these businesses. You may contact your manager regarding GLB training opportunities.

VIII. The Foreign Corrupt Practices Act

The U.S. Foreign Corrupt Practices Act, as amended by the International Anti-Bribery and Fair Competition Act of 1998 (FCPA), makes it a crime to bribe officials of another country. The law applies to U.S. companies and their domestic and foreign subsidiaries, and their employees or agents (whether or not U.S. nationals), as well as other foreign persons who violate the law in the U.S. The FCPA has two basic parts: (1) anti-bribery provisions, and (2) accounting and record-keeping requirements.

The anti-bribery provisions make it illegal to bribe a foreign public official, political party, party official or candidate for political office, or an official of a public international organization. The FCPA defines a “bribe” as any payment, directly or indirectly, or any offer or promise to pay, anything of value (whether cash or otherwise) to the recipient for the purposes of influencing or rewarding an act or decision to obtain, retain or direct business, or for the purpose of obtaining any “improper advantage” (e.g., tax breaks, immunities, permits or priorities not otherwise earned). The FCPA’s accounting and record-keeping provisions require companies to keep detailed corporate books, records and accounts, and prohibits the falsification of those materials. The accounting and record-keeping provisions apply to domestic as well as foreign operations of publicly traded U.S. companies. These requirements complement the anti-bribery provisions by preventing the creation of unreported slush funds for illegal payments. It is important to understand that the law requires strict accuracy in documentation and reporting. These provisions can be interpreted to include relatively small sums from petty cash funds.

Consistent with the FCPA, Equifax corporate policy requires that:

- No Company employee or agent will pay or offer a “bribe” as defined in the FCPA;
- No Company employee or agent will establish any undisclosed or unrecorded fund of cash or assets for any purpose, or make any false, artificial, or misleading entries in any books or records of Equifax;
- No Company employees or agents will approve or make any payment for any purpose other than that described by the document supporting the payment; and the Company Chief Financial Officer or his/her written designee must provide prior written approval before a Company employee or agent:
- Makes any payment or gift foreign public or party officials, international public officials or foreign political candidates of more than a nominal value;
- Pays travel or lodging expenses of, or makes any substantial entertainment expenditure for, any of those officials;
- Makes any “facilitating or grease payments” to facilitate routine governmental action of more than a nominal value;
- Makes contributions to campaigns of foreign political parties, officials or candidates;
- Engages an agent, consultant, or advisor who may have dealings with foreign governments or political parties on behalf of Equifax; or makes any payment arrangements where a person performing services or selling goods in one country requests that payments be made in another country (“split payments arrangements”).



Anyone who is convicted of violating the FCPA is subject to substantial fines or imprisonment.

IX. Conflicts of Interest

We expect Equifax officers and employees to avoid any activity, investment, interest or association that interferes or appears to interfere with their independent exercise of judgment in carrying out an assigned job responsibility, or with the interests of Equifax and its shareholders as a whole. Conflicts of interest may arise in many situations. They occur most often where an employee or his/her family members obtain some personal benefit at the expense of the Company.

If there are any questions whether or not a specific act or situation represents, a conflict of interest, or if you suspect a conflict of interest exists, you should consult your supervisor or the Code of Conduct Compliance Officer before undertaking the action or creating the potential conflict situation.

Some of the most common conflict situations are:

- *Outside Financial Interests:* No employee will have a significant financial interest, either directly or indirectly, in any supplier, contractor, customer or competitor of the Company, or in any business transaction involving the Company, without full disclosure to and written clearance from the Code of Conduct Compliance Officer;
- *Doing Business with Relatives:* No Employee will engage in any business transaction on behalf of the Company with a relative by blood or marriage, or with a firm of which that relative is a principal, officer or representative, without prior full disclosure to and written clearance from an appropriate Company officer; and
- *Use of Company Property:* No employee will use Company property and services for their personal benefit unless use of that property and those services has been properly approved for general employee or public use. You must obtain prior Company approval for the use of Company-owned land, materials, equipment, etc., under any other circumstances. You must not sell, lend, give away or otherwise dispose of Company property, regardless of condition or value, without proper authorization.
- *Loan and Advances to Directors and Executive Officers.* Equifax is prohibited from extending or maintaining credit, or arranging for the extension or renewal of an extension of credit, in the form of a personal loan, to any Equifax director or executive officer. Extensions of credit for non-executive officer employees shall be made in accordance with any other Company policy related to these matters.
- *Corporate Opportunities.* Officers and employees are prohibited from (a) taking for themselves personally opportunities that are discovered through the use of Company property, information or position; (b) using Company property, information, or position for personal gain; and (c) competing with the Company. Officers and employees owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises.

X. Relationships With Suppliers/Contractors/Customers

Dealing with suppliers, contractors and customers may be sensitive involving issues of law and ethics. In general, Equifax expects that all its employees shall conduct business honestly and ethically. The following guidelines supplement, but do not replace, specific criteria in the Company's purchasing or sales policies:

- *Treatment of Others:* Employees must treat all suppliers, contractors and customers fairly and honestly at all times. These parties should not be taken unfair advantage of through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair dealing.
- *Accepting or Giving Money, Gifts or Entertainment:* No employee, personally or on behalf of the Company, will directly or indirectly request, accept, offer or give money, gifts of other than nominal value, unusual hospitality or entertainment, loans (except from lending institutions) or any other preferential treatment in dealing with any present or potential Equifax supplier, contractor, customer or competitor.
- *Payment to Purchasing Agents:* No employee, personally or on behalf of the Company, will make payments to purchasing agents or other employees of any supplier, contractor or customer to either obtain or retain business, or to realize higher or lower prices for the Company. However, you may give gifts of nominal value on customary gift-giving occasions.

- **Special Requirements for Government Contracts.**

The Company provides products and services under several contracts with federal and state government agencies. Employees who are involved with those contracts must be careful to follow additional rules that apply to government contracts. Some of those rules are as follows:

- It is illegal under both U.S. federal and state law to solicit, offer, or pay any bribe or other gratuity to a public official for the purpose of influencing an official act or decision;
- It is illegal under the U.S. federal False Claims Act to file a false report or make any false statement for the purpose of either making a claim for payment from the government, or avoiding a specific payment obligation to the government.

XI. Records Retention/Destruction

The Company's corporate records are important assets. Corporate records include essentially all records you produce as an employee, whether hard copy or electronic. A record may be as obvious as a memorandum, an e-mail, a contract or a case study, or something not so obvious, such as a computerized desk calendar, an appointment book, or an expense record. 16

The law requires us to maintain certain types of corporate records, usually for a specified period of time. Failure to retain those records for those minimum periods could subject the Company to penalties and fines, cause the loss of rights, obstruct justice, place the Company in



contempt of court, or seriously disadvantage the Company in litigation.

From time to time the Company establishes retention or destruction policies or schedules for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management. We expect all employees to fully comply with any published records retention or destruction policies and schedules.

- **Litigation Exception.**

If you believe, or the Company informs you, that Company records in any form are relevant to litigation or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until the Legal Department or Compliance Officer determines the records are no longer needed. This exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that this exception may apply, or have any question regarding the possible applicability of that exception, please contact your supervisor, the Legal Department or the Code of Conduct Compliance Officer.

XII. Antitrust and Trade Regulation

Equifax complies fully with the letter and the spirit of all applicable laws governing antitrust and trade regulation. Those laws are designed to ensure free and open competition in the marketplace by prohibiting any activities that unfairly or unreasonably restrict normal competition. The antitrust laws of the U.S. and other countries prohibit, under various circumstances, activities such as price fixing, territorial divisions, unfair price discrimination, monopolizing trade, unreasonably refusing to deal with a particular customer or vendor, and “tying” arrangements where a customer is required to buy one product or service in order to obtain another product or service.

Antitrust violations can subject both the employee and the Company to substantial penalties, including civil, criminal, and disciplinary action or discharge from the Company. Although it is impossible to list all possible examples of antitrust violations, the following rules demonstrate the types of activities that you should avoid:

- *Relations with Competitors:* Equifax employees must not participate in any arrangement with competitors to fix prices. Examples of price fixing include rigged or coordinated bidding and the systematic exchange of price information.
- You must not take any action with competitors to divide or allocate markets, or to mutually refuse to deal with third parties. To avoid the appearance of these activities, employees must be careful to limit the exchange of information with our competitors;
- *Relations with Customers:* Our employees must not require our customers to resell our product or services at specified resale prices or at prices exceeding specified minimums. (That restriction generally does not apply to agents selling our products or services on our behalf.) Under certain circumstances it may be unlawful to prohibit our customers from buying products or services from other suppliers. Although the Company has a broad right to select the customers with whom it wants to do business,

that right must be exercised with caution, and any refusal to deal with a particular customer must be evaluated carefully;

- *Relations with Suppliers:* We must not enter into agreements with our suppliers to resell their products or at prices exceeding specified minimums. Also, under certain circumstances, we may not enter into agreements with suppliers prohibiting them from selling to competitors of the Company; and
- *Trade Associations:* When representing the Company in trade association activities, employees must be careful not to share pricing or other non-public competitive information, or engage in any other activity that could reasonably be construed as price fixing or in restraint of trade.

In addition to complying with U.S. and foreign antitrust laws, Equifax employee must comply with a number of laws governing trade regulation in general. Those laws require that all employees refrain from any unfair or deceptive methods of competition, including false or misleading advertising, making false statements concerning competitors or their products, and inducing our competitors' customers or employees to breach their contracts with our competitors. Contact the Legal Department of the Code of Conduct Compliance Officer if you have any questions about what type of activities would be considered to violate antitrust or trade regulation laws.

XIII. Insider Information and Securities Trading

- **Material nonpublic information must be kept confidential and not used.**

As a publicly traded company, Equifax is required to provide full and fair public disclosure on a timely basis of various "material nonpublic" information, as defined below. In the course of business, some employees may have access to such material information before it becomes public knowledge. Until it is released to the public, material information must be kept confidential. Use of material information that is not publicly known for personal gain, or the release of that information to others who may use it for personal gain, ("insider trading," as defined below) is considered to be fraud against the Company and against other members of the investing public who are disadvantaged because they do not have access to the information.

An employee who does so is in violation of U.S. law and Company policy.

- **Material nonpublic information defined.**

Information is generally considered to be "**material**" if a reasonable investor would likely consider it to be important in making his or her investment decision, or if the release of the information is reasonably certain to have an effect on the price of the Company's stock. Information you should consider material includes, but is not limited to: a pending stock split, dividend changes, earnings estimates, changes in previously released earnings estimates, significant merger or acquisition proposals or developments, major litigation, the acquisition or loss of a major contract, and extraordinary management developments.

Information is "**nonpublic**" until it has been communicated to the stock market and the public, and they have had time to "absorb" the information. For example, information

found in a report filed with Securities and Exchange Commission, or appearing in *The Wall Street Journal* or other publications of general circulation, would be considered public. As a rule of thumb, the market has had time to absorb information that has been public for two full business days.

- **Insider trading defined.**

“Insider trading” refers to the improper use of material nonpublic information, including:

- Trading by an insider (defined below), while aware of material nonpublic information;
- Trading by a non-insider, while aware of material nonpublic information, where the information either was disclosed to the non-insider in violation of an insider’s duty to keep it confidential or was misappropriated; or
- Communicating material nonpublic information to others whose jobs do not require them to have the information to enable them to trade on that information (tipping).
- Persons who are not related to the Company but who are not tipped material nonpublic information and trade may also be committing a crime.

The concept of “*insider*” is broad. It includes Company officers, directors and employees, and “temporary insiders” who enter into a special confidential relationship in the conduct of the Company’s affairs and are given access to material nonpublic information. A temporary insider can include Equifax’s attorneys, accountants, consultants, bank lending officers, and the employees of those parties.

- **Insider trading is a serious crime.**

Penalties for trading on or communicating material nonpublic information are severe, both for individuals involved in the lawful conduct and their employers. Where a violation occurs, a person can be subject to substantial penalties, including civil liability, criminal liability, and disciplinary action or termination of employment, even if they do not personally benefit from the violation.

- **Guidelines for compliance.**

The following guidelines should help you comply with the rules regarding insider trading:

- You must not share material nonpublic information with those people inside Equifax whose job do not require them to have the information;
- You must not disclose any material nonpublic information to anyone outside the Company except in accordance with Equifax’s standard procedures for the release of nonpublic information; and when you have material nonpublic information regarding Equifax (or material nonpublic information regarding any other publicly traded company that you have obtained as a result of your employment with Equifax) you must not buy or sell, or advise anyone else to buy or sell, the securities of Equifax or any other company that might be materially affected by the information, until that information is disclosed to the public and absorbed by the market.



Contact either the Code of Conduct Compliance Officer or the General Counsel if you have any questions about what type of information is considered material nonpublic information.

XIV. Media Relations

In all our dealing with the press and other media, the Company must speak with a unified voice. Accordingly, except as otherwise designated by the Company's Chief Executive Officer, Corporate Public/Media Relations is the sole contact for media seeking information about Equifax. Any requests from the media must be referred to Public/Media Relations. They will deal directly with the media and make appropriate arrangements. Public/Media Relations must approve any articles, press release, or other public communication involving the Company prior to publication.

XV. Advertising and Statements to Customers

All of our advertising, representations and claims about products or services must be truthful and not deceptive. False, misleading or unfair comparisons with, or claims concerning, the products or services of others may be considered deceptive, and you must avoid them.

XVI. Confidential Information and Intellectual Property

- **Confidential Information**

One of the Company's most valuable assets is its body of business information, which includes information that is generally not known to the public or our competitors, and which would harm the Company if it were disclosed inappropriately. Failure to adequately protect this confidential information could place Equifax at a disadvantage in the marketplace.

As an Equifax employee, you are responsible and accountable for the integrity and protection of the Company's confidential information, and you must take all reasonable precautions to protect this information from improper disclosure. You must not disclose confidential information except when it is necessary and appropriate in connection with your responsibilities. You should handles carefully any documents containing confidential information during working hours, and properly secure them at the end of the business day. You should pay particular attention to the security of data stored on your computer systems. You must maintain the secrecy of all computer systems, and secure any equipment when not in use.

- **Intellectual Property**

The Company's intellectual property includes inventions, improvements, ideas, information, software, models and programs, together with the related materials, documentation, patents, trademarks, copyrights, and other rights that go along with them. Equifax will normally be the exclusive owner of all rights in intellectual property that is related to our businesses or is developed by our employees and contractors in the course of their employment or service with Equifax. This is true whether or not the employees or contractors make the developments during working hours, on Company premises, or using Company material or resources.

Equifax's intellectual property rights are extremely valuable to the Company. They are also extremely "fragile," because they can be compromised or even forfeited if we do not vigilantly protect them. In order to protect the Company's intellectual property, all Equifax employees and contractors should use their best efforts to:

- Recognize and identify the Company's actual or potential intellectual property assets;
- Notify the appropriate Equifax personnel (either a senior technology officer, the Legal Department or the Code of Conduct Compliance Officer) of the existence and development of intellectual property assets;
- Assist in securing Equifax's ownership of intellectual property assets;
- Assist, where appropriate, in registering, patenting, or otherwise legally protecting intellectual property assets;
- Use the intellectual property assets properly, including in licensing and other transactions;
- Prevent any infringement or misuse of the Company's intellectual property;
- Notify the appropriate Equifax personnel (your manager, the Legal Department or the Code of Conduct Compliance Officer) of any potential infringement or misuse of the Company's intellectual property, so that we may take appropriate action; and
- Have outside vendors, contractors, licensees, joint venture partners and employees sign the appropriate Equifax documents acknowledging Equifax's intellectual property ownership.

- **Rights of Others**

Equifax employees and contractors also must ensure that they do not misuse the intellectual property or confidential information of any other parties. There are several U.S. federal and state laws that prohibit the theft or unauthorized use of the intellectual property or confidential information of others. Violations of those laws can result in substantial fines or imprisonment. When new employees are hired, it is especially important to ensure that they do not improperly disclose any confidential information of others to the Company or use others' intellectual property for the Company's advantage.

Remember:

If you have question about the Code, consult with your supervisor, the Human Resources Department or the Company's Code of Conduct Compliance Officer.

You are responsible for reporting any events, practices or circumstances that you suspect may violate the Code, including applicable laws and regulations. You may report such activity to any of the following persons:

- **Your supervisor**
- **Human Resources Representative**
- **Company's Code of Conduct Compliance Officer by any of the following methods:**
 - In writing, addressed to the Code of Conduct Compliance Officer, either by internal mail to: Mail Drop H-53 or by U.S. mail to Equifax, 1550 Peachtree Street, NW, Atlanta, GA 30309
 - **By e-mail** to "Code of Conduct Compliance Officer" or by Internet at codeofconduct.office@equifax.com
 - **By phoning** the Equifax Reporting Line:(877) 482-5252. For international locations, please refer to Equifax Central (Ethics section) for your access code when dialing.

You are responsible for reporting any events, practices or circumstances that you suspect may violate the Code, including applicable laws and regulations. You may report such activity to any of the following persons:

- **General Counsel, in the case of questionable accounting, internal control or auditing matters.**

You may also be permitted to report to other appropriate persons if so specified in this Manual or in auditing matters.

You may report anonymously to the Code of Conduct Compliance Officer or General Counsel. Do not e-mail them if you wish to remain anonymous; contact them by mail or through the Equifax Reporting Line.