



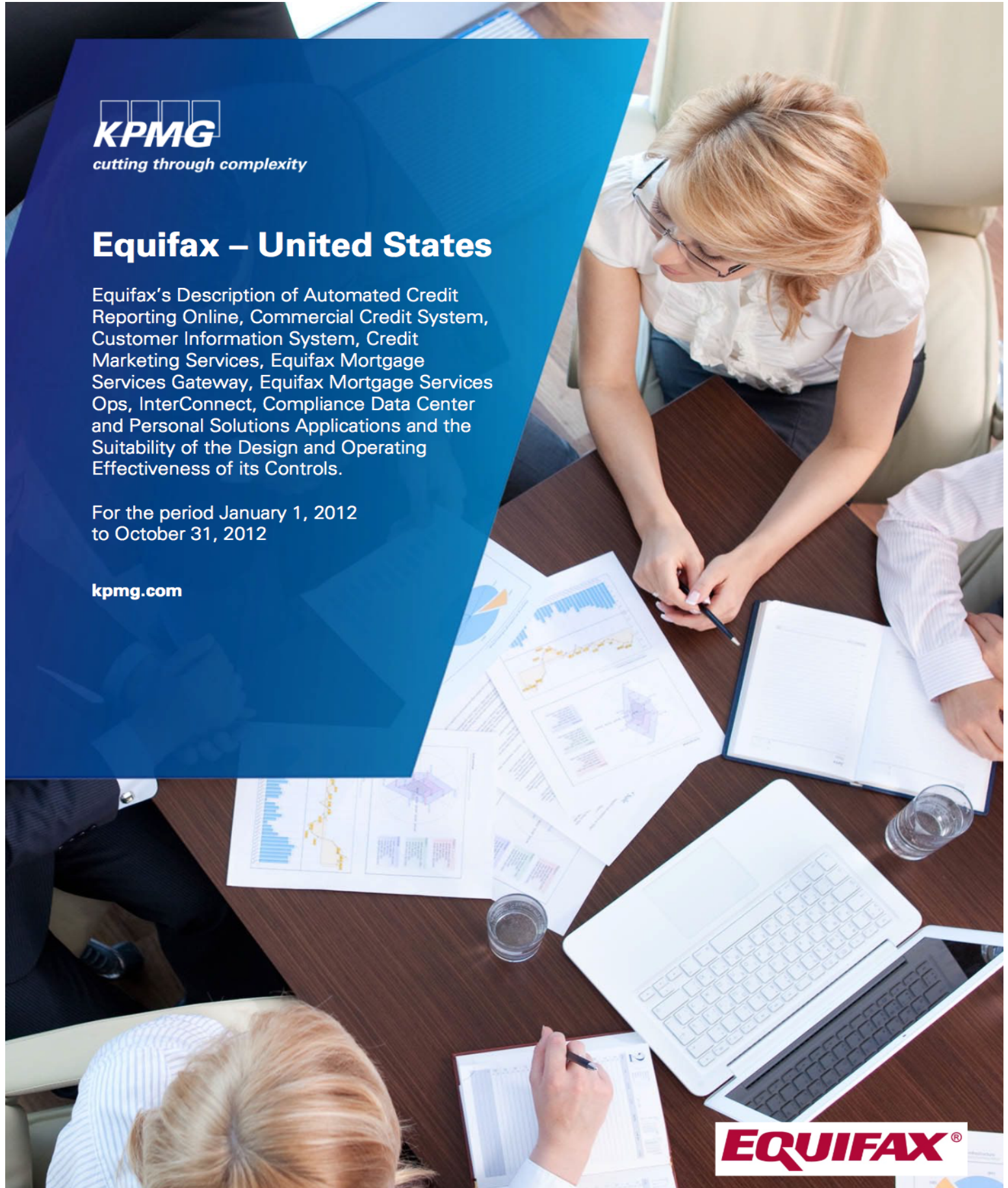
cutting through complexity

Equifax – United States

Equifax’s Description of Automated Credit Reporting Online, Commercial Credit System, Customer Information System, Credit Marketing Services, Equifax Mortgage Services Gateway, Equifax Mortgage Services Ops, InterConnect, Compliance Data Center and Personal Solutions Applications and the Suitability of the Design and Operating Effectiveness of its Controls.

For the period January 1, 2012 to October 31, 2012

kpmg.com



**EQUIFAX AUTOMATED CREDIT REPORTING ONLINE, COMMERCIAL CREDIT SYSTEM,
CUSTOMER INFORMATION SYSTEM, CREDIT MARKETING SERVICES, EQUIFAX
MORTGAGE SERVICES GATEWAY, EQUIFAX MORTGAGE SERVICES OPS,
INTERCONNECT, COMPLIANCE DATA CENTER AND PERSONAL SOLUTION
APPLICATIONS**

**Report on Equifax's Controls Placed in Operation and Tests of Operating Effectiveness
For the Period January 1, 2012 through October 31, 2012**

Table of Contents

Section I.	Independent Service Auditor's Report Provided by KPMG LLP	
Section II.	Equifax and IBM's Assertion	
Section IIa.	Equifax's Assertion	
Section IIb.	IBM's Assertion	
Section III.	Description of Controls Provided by Equifax Commercial Information Solutions, Consumer Information Solutions, Mortgage Services, Personal Solutions, and Technology and Analytical Services – Untied States	
	Overview of Company and Services.....	16
	Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication	21
	Control Environment	21
	Organization	21
	Risk Assessment Process	23
	Monitoring	24
	Information and Communication.....	24
	Description of General Computer Controls	26
	Control Objective 1: Systems Development and Maintenance	26
	Control Objective 2: Data Center Physical Security.....	32
	Control Objective 3: Logical Security	34
	Control Objective 4: Job Scheduling and Problem Management	38
	Control Objective 5: Network Performance & System Capacity Monitoring	40
	Control Objective 6: Backups.....	40
	Complementary User Entity Controls.....	42

Equifax's control objectives and related controls are included in Section IV of this report, Equifax's Control Objectives and Related Controls, and KPMG LLP's Tests of Controls and Results of Tests." Although the control objectives and related controls are presented in Section IV, they are, nevertheless, an integral part of Equifax's description of its system as described in Section III.

Section IV. Equifax's Control Objectives and Related Controls, and KPMG LLPs Tests of Controls and Results of Tests

Use of Internal Audit 44

Equifax's Control Objectives and Related Controls and KPMG LLP's Tests of Controls and Results of Tests 45

Section V. Other Information Provided by Equifax Inc.

Revenue, Business Continuity and Disaster Recovery Program, Insurance Coverage..... 70

Section I
Independent Service Auditors' Report
Provided by KPMG LLP



KPMG LLP
Suite 2000
303 Peachtree Street, N.E.
Atlanta, GA 30308-3210

Independent Service Auditors' Report

The Board of Directors
Equifax Inc.:

Scope

We have examined Equifax Inc.'s (Equifax) and International Business Machines Corporation, Global Technology Services (IBM) description of their Information Technology General Controls for Automated Credit Reporting Online, Commercial Credit System, Customer Information System, Credit Marketing Services, Equifax Mortgage Services Gateway, Equifax Mortgage Services Ops, InterConnect, Compliance Data Center and Personal Solutions applications throughout the period January 1, 2012 to October 31, 2012 (description) and the suitability of the design and operating effectiveness of Equifax's and IBM's controls to achieve the related control objectives stated in the description. IBM is an independent service organization that provides certain computer operations and infrastructure support services to Equifax. Equifax's description includes a description of IBM used by Equifax to process transactions for its user entities, as well as relevant control objectives and controls of IBM. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Equifax's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or the operating effectiveness of such complementary user entity controls.

The information in section V of management's description of the service organization's system, "Other Information Provided by Equifax, Inc.," that describes Revenue by segment and Business Continuity, and insurance coverage is presented by management of Equifax to provide additional information and is not a part of Equifax's description of its system made available to user entities during the period January 1, 2012 to October 31, 2012. Information about Revenue, Business Continuity, and insurance coverage has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system, and, accordingly, we express no opinion on it.

Service organization's responsibilities

In their description, Equifax and IBM have provided their assertions about the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description. Equifax and IBM are responsible for preparing the description and for the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting and using suitable criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.



Service auditors' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, the controls were suitably designed and the controls were operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2012 to October 31, 2012.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and the operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization or subservice organization may not prevent, or detect and correct, all errors or omissions in transaction processing. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or subservice organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in Equifax's and IBM's assertions, (1) the description fairly presents Equifax's Information Technology General Controls for the in-scope applications and the Transaction Processing Controls for the Customer Information System and Credit Marketing Services applications and IBM's computer processing services used by Equifax to process transactions for its user entities were designed and implemented throughout the period January 1, 2012 to October 31, 2012, (2) the controls related to the control objectives of Equifax and IBM stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2012 to October 31, 2012, and (3) the controls of Equifax and IBM that we tested, which together with the complementary controls at user entities referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description in section III were achieved, operated effectively throughout the period January 1, 2012 to October 31, 2012.

Description of tests of controls

The specific controls and the nature, timing, extent, and results of the tests are listed in section IV.



Restricted use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of Equifax and user entities of Equifax's Information Technology General Controls for the in-scope applications during some or all of the period January 1, 2012 to October 31, 2012, and the independent auditors of user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

January 7, 2013

Section II

Equifax and IBM Assertions

Section IIa **Equifax's Assertion**



We have prepared the description of Equifax, Inc's (Equifax) general computer controls applicable to the processing of transactions of Information Technology General Controls for Automated Credit Reporting Online, Commercial Credit System, Customer Information System, Credit Marketing Services, Equifax Mortgage Services Gateway, Equifax Mortgage Services Ops, InterConnect, Compliance Data Center and Personal Solutions applications and Transaction Processing Controls for the Customer Information System and Credit Marketing Services applications (the System) for user entities of the system during some or all of the period January 1, 2012 to October 31, 2012, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief that:

- a) The accompanying description in Section III and IV fairly presents the general computer controls applicable to the processing of transactions of the System made available to user entities of the System during some or all of the period of January 1, 2012 to October 31, 2012. Equifax uses an independent service organization, International Business Machines Global Technology Services (IBM) to provide certain computer operations and infrastructure support services. The description in Sections III and IV includes both the controls and related control objectives of Equifax, and the control objectives and related controls of IBM. The criteria we used in making this assertion were that the accompanying description:
 - i. Presents how the relevant general computer controls and application processing controls of the System were designed and implemented to support the processing of relevant transactions, including:
 - The types of services provided by the System including, as appropriate, the classes of transactions processed;
 - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
 - How the System captured and addressed significant events and conditions, other than transactions.
 - Specified control objectives and controls designed to achieve those objectives;
 - Controls that we assumed, in the design of the System, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and

- Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.
- ii. Does not omit or distort information relevant to the scope of the System being described, while acknowledging that the description was prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own environment.
- b) The description includes relevant details of changes to the System during the period covered by the descriptions.
 - c) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period January 1, 2012 to October 31, 2012 to achieve those control objectives. The criteria used in making this assertion were that:
 - i. The risks that threatened achievement of the control objectives stated in the description were identified;
 - ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Equifax Inc.
January 7, 2013

Section IIb

IBM's Assertion



January 7, 2013

We have prepared the description of IBM's system of common controls for multiple customers (the "IBM Controls" identified below) provided for Equifax's Automated Credit Reporting Online, Customer Information System, Credit Marketing System, Commercial Credit, Equifax Mortgage Services Gateway, Equifax Mortgage Services Ops, InterConnect, Compliance Data Center and Personal Solutions system (the System) for user entities of the System during some or all of the period January 1, 2012 to October 31, 2012 and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, to understand the nature of the controls that are the subject of this report and any role such other information and/or controls may play in such user entity's overall control structure when assessing the risks of material misstatements of user entities' financial statements.

The data center that contains the System is in Alpharetta, Georgia and is on the premise of Equifax at its Alpharetta headquarters location. IBM provides personnel who perform services for Equifax based on a contractual arrangement.

For the purposes of the description, IBM designed and performed certain controls as follows (numerical references are identified within the matrices in Section IV of this report):

- IBM has designed and operated the following controls (the "IBM Controls"):
 - Control 5.01 (The IBM Network Monitoring Center is responsible for monitoring network performance for the in-scope applications throughout the day using network monitoring systems to identify process and batch run performance issues, CPU and memory utilization issues, failed system connections, and backup performance issues).
 - Control 5.02 (IBM prepares a report of network performance trends that is shared at monthly meetings between IBM and Equifax. The report includes root cause analyses for major outages occurring during the month).
- Equifax is responsible for the design of all controls other than the IBM Controls. With the exception of controls 2.01, 2.02, 2.03 3.04, 5.03 and 5.04, IBM operated the remainder of the Equifax controls itself or jointly with Equifax.

We confirm, to the best of our knowledge and belief that:

- a) The accompanying description of the IBM Controls in Sections III and IV of this report as it relates to IBM provided services as noted above, fairly presents in all material respects those aspects of the IBM Controls that we believe are likely to be relevant to user entities in assessing their own internal controls to the extent that the IBM Controls were made available to user entities of the System during some or all of the period January 1, 2012 to October 31, 2012 for processing their transactions. The criteria we used in making this assertion were that the accompanying description:
 - i. Presents how the IBM Controls made available to user entities of the System were designed and implemented to the extent they relate to the processing of relevant transactions, including:
 - The procedures, within both automated and manual systems, by which services are provided, to the extent they relate to the IBM Controls;

- How the system captured and addressed significant events and conditions, other than transactions;
 - Specified control objectives and controls designed to achieve those objectives;
 - The role of certain aspects of applicable, complementary Equifax and user entity controls contemplated in the design of the service organization's controls, as more specifically described in Sections IIb, III, and IV; and
 - Certain other aspects of our control environment, risk assessment process, information and communication, control activities and monitoring controls that we believe were relevant to the IBM Controls.
- ii. The description of the IBM Controls was prepared to meet the common needs of a broad range of user entities and their independent auditors and may not, therefore, include every aspect of the IBM Controls that each individual user entity may consider important in its own particular environment.
- b) The description includes relevant details of changes to the IBM Controls during the period covered by the descriptions.
- c) The IBM Controls were suitably designed and operated effectively throughout the period January 1, 2012 to October 31, 2012 to achieve the control objectives specified by IBM. The criteria used in making this assertion were that:
- i. The risks that threatened achievement of the control objectives stated in the description of the IBM Controls were identified;
 - ii. The identified IBM Controls would, if operated as described, provide reasonable, but not absolute, assurance that those risks did not prevent the stated control objectives from being achieved; and
 - iii. The IBM Controls were consistently applied by individuals who have the appropriate competence and authority.
- d) To the extent that IBM operated the Equifax controls, those controls operated effectively as described in this report throughout the period January 1, 2012 through October 31, 2012, provided that (i) where Equifax had responsibilities with respect to such controls, it did not do or fail to do anything that would have caused them not to operate effectively, and (ii) for purposes of this statement, "effectively" has the same meaning that it has for those controls operated and designed solely by Equifax.

The assertions and other statements contained herein do not (i) amend any agreement between IBM and any customer or user organization or their respective rights and obligations under any agreement to which the controls described herein relate or create any rights or causes of action under any such agreement or otherwise, or (ii) substitute for any independent analysis or verifications otherwise required of a user entity or its representatives. IBM makes no representation or warranty regarding (i) the adequacy of controls required by any party or (ii) to the design of any control other than the IBM Controls or, except to the extent expressly indicated in (d) above, the operating effectiveness of any controls other than the IBM Controls, or (iii) to the adequacy, effectiveness or significance of the System or the design or effectiveness of any specific controls and with respect to ultimate assessments of control risk at user entities, which are dependent on their interaction with the controls and other factors present at or implemented by individual user entities. User entities retain ultimate authority and responsibility for determining whether controls used or implemented by them are relevant to or sufficient for their needs.

Section III

Description of Controls Provided by Equifax

Overview of Company and Services

SCOPE OF REPORT

The scope of this report covers Information Technology (IT) General Controls related to Equifax's Automated Credit Reporting Online (ACRO), Commercial Credit System (CCS), Customer Information System (CIS), Credit Marketing Services (CMS), Equifax Mortgage Services Gateway (EMS Gateway), Equifax Mortgage Services Ops (EMS Ops), InterConnect, Compliance Data Center (CDC) and Personal Solutions (PSOL) applications, hosted in Alpharetta, Georgia, and select Transaction Processing Controls related to Equifax's Customer Information System and Credit Marketing Services applications. This report does not apply to any other applications, products, or services provided by Equifax.

Additionally, certain computer applications are referenced within the 'Description of Controls' that are not included within the scope of the examination. Specifically, the Accounts Payable, Accounts Receivable, Apply Systems, Bureau Statistics, Criteria Automation Package, ePORT, General Ledger, Deal Manager, and Price List Database applications.

OVERVIEW OF OPERATIONS

Description of Equifax Inc.

Equifax Inc. (Equifax), which is headquartered in Atlanta, Georgia, provides credit services throughout the United States to banks, retailers, finance companies, commercial lenders, financial services organizations, and other credit grantors.

Description of Equifax Information Technology

Software development and maintenance for ACRO, CCS, CIS, CMS, CDC EMS Gateway, EMS Ops, and PSOL is performed by Equifax Information Technology (EIT). Software development and maintenance for the InterConnect application is performed by Equifax Technology and Analytical Services (TAS).

The computer processing environment for all of the applications relevant to this report is supported by mainframe and midrange computers, which are located in an Equifax data center in Alpharetta, Georgia. The maintenance and operation of the mainframe, components of the midrange, and components of the network infrastructure are outsourced to IBM Global Technology Services (IBM). Equifax retains responsibility for the confidentiality and integrity of its data and therefore maintains sole control of the information security policy, information security organization, security architecture, and governance required to protect the data.

The responsibilities of IBM that are included in this report include the operation of certain controls related to: Systems Development and Maintenance, Data Center Physical Security, Logical Security, Job Scheduling and Problem Management, Network Performance Monitoring, and Backups. The responsibilities of IBM not included in this report are: computer hardware and support maintenance, disaster recovery, and data center environmental controls.

OVERVIEW OF APPLICATION SYSTEMS

ACRO is the core system for EIS processing and is the data source of credit information used to develop the variety of products provided through the in-scope systems. ACRO uses automated interfaces with Customer Information System (CIS) to perform billing functions as detailed below. Management performs periodic comparisons between transaction billing and in-scope systems. ACRO accounts for more than 50% of the total transaction volume (See Section IV). The other in-scope systems provide for customer and data interfaces for the provisioning of customer services provided by EIS to its clients.

Automated Credit Reporting On-line

ACRO provides credit reports, scores, decisions, account management, identification-location, collections, utility-telecommunications, and prescreen products. Credit reports are billed and accounted for through an automated interface with the CIS, which performs rating and billing functions.

ACRO is developed and maintained by US Consumer Information Solutions IT team, which is part of EIT. ACRO is processed on an IBM mainframe, running the z/OS operating system.

Commercial Credit System

Commercial Information Solutions combines banking and leasing payment information with trade credit history to produce reports that help customers better understand and manage the financial risk of doing business with small businesses by providing data that can help customers assess credit risk. Reports are distributed through ePORT, InterConnect, and Apply applications. Reports delivered through these services are inquiry only. The ePORT and Apply applications were excluded from the scope of this examination, and accordingly, KPMG expresses no opinion on internal controls related to these applications.

The CCS application is maintained by the North American Commercial Solutions IT team, which is part of EIT. CCS is the repository for the data provided by the Small Business Financial Exchange and Small Business Exchange. Member companies contribute the credit performance of their accounts to CCS. The CCS application edits the data and loads it into the Commercial Credit Database. Other data types such as firmographics, public records, and bankruptcy are also loaded into the database. Commercial Credit operates on Solaris UNIX servers and data is stored in Oracle and DB2 databases.

Compliance Data Center System

CDC maintains a comprehensive compliance database with data from multiple sources of information, including various government and agency lists worldwide, and global media reports of white-collar criminal activity and terrorist-related activities.

The primary applications that support CDC are GreyCon, Midrange, and eCrunch. The CDC GreyCon application is a client server, asynchronous state, transaction processing system that is used to manage the CDC database. The CDC eCrunch application is a desktop client application that is used by CDC Information Analyst to confirm CDC Alerts prior to customer delivery. The CDC Midrange application is the core engine used to generate the Alert files and update customer portfolios.

CDC reviews billing information for each customer with CDC Pricing Support Personnel to verify pricing details. These amounts are entered into billing records each month. The billing process utilizes the transaction counts for all customers and creates monthly invoices for customers.

Access to the CDC platform primarily allows processing of files delivered via the Equifax FTP Service. Additionally, an interface is provided to the Equifax InterConnect applications for individual transaction processing. The controls for the Equifax FTP Service and Equifax NexGen applications are not included in the scope of this document.

The CDC platform utilizes Oracle databases and file-servers and is supported by multiple clusters of Sun servers, running the Solaris operating system and Intel servers, running Microsoft Windows operating system. The system is divided into internally redundant functional clusters with a modular design. The separate clusters are:

- Legacy
- Midrange Application Servers
- Client Application Servers
- Database Servers

The CDC application was developed and is maintained by North American Commercial Solutions IT team, which is part of EIT personnel.

Customer Information System

The Customer Information System (CIS) and related billing processes support the following functions:

- Create, populate, and validate customers and two level of families separately for pricing, billing and reporting;
- Prepare a daily upload of customer and family information to ACRO and other USA/Canadian systems;
- Maintains real-time synchronization between ACRO USA and ACRO Canada databases with CIS for customer information, activation status and other information. Provides ACRO USA database with customer security initialization.
- Combine duplicate inquiries based on updated business rules and extract errors for correction;
- Maintain and provide pricing, taxing, revenue sharing, and product information;
- Maintain and archives “unbilled business” for cycle invoicing and financial system uploads;
- Invoices 4 times a month in paper, magnetic media, and internet
- Prepare affiliate net bills and revenue reports;
- Compute royalty payments to third party data or model providers;
- Generate financial, product, company, sales point, and customer reports;
- Gather and prepare daily billing transactions for nightly processing; and

- Prepare financial information for transfers to Accounts Receivable, Accounts Payable, and the General Ledger.

CIS is maintained by the Global Corporate Platforms IT team, which is part of EIT, for change control, technical specification, and QA. It is processed on an IBM mainframe, running the z/OS operating system, and utilizing the IBM DB2 relational database management system and related infrastructure, tools, and components.

Credit Marketing Services System

The Credit Marketing Services System utilizes a copy of the ACRO database to develop lists of customers for credit marketing and account analysis purposes. The CMS data resides on an IBM mainframe, running the z/OS operating system. After the lists are created, the number of names is passed to the CMS application for customer billing and also for revenue sharing among the file owner and file seller.

CMS performs the calculations and allocations of revenue to sales points for promotional lists. The CMS application downloads the summary name count by sales point data. Then the cost and rating data is manually input into CMS to allow CMS to allocate the costs and calculate net revenue, a per-name rate, and revenue for sales points (office where sale is initiated).

CMS is maintained by the Global Corporate Platforms IT team, which is part of EIT. The CMS application utilizes Oracle Financials™ software, which runs on IBM RS-6000 servers, running the AIX UNIX operating system, and utilizes an Oracle relational database.

Equifax Mortgage Services Gateway and Ops Systems

Equifax Mortgage Services (EMS) is a fully integrated service that offers a variety of credit-related services focused on the mortgage industry, including credit reporting, risk scoring, fraud protection, portfolio management, and prescreen services.

The EMS Gateway application is Equifax's online platform that supports Equifax Mortgage Services. The EMS Gateway application is a client server, asynchronous state, transaction processing system that generates merged mortgage credit reports, such as Credit*Hi-Lites® (CHL's), Edited Credit*Hi-Lites (ECHL's), and Residential Mortgage Credit Reports (RMCR's). The EMS Ops application is used to maintain the pricing data for EMS Gateway and sends billing transaction data to CIS on a nightly basis.

The EMS Gateway and EMS Ops applications utilize Informix and Oracle databases and are supported by multiple clusters of IBM RS-6000 servers, running the AIX UNIX operating system. The system is divided into internally redundant functional clusters with a modular design. There are three separate clusters:

- Gateway Application Servers
- EMS Operations (EMS Ops)
- Database Servers

The EMS Gateway and EMS Ops applications are supported by US Consumer Information Solutions IT team, which is part of EIT. All Mortgage Gateway billing is processed through CIS.

InterConnect

InterConnect is a business-to-business decision platform that supports real-time decisions and task management. InterConnect receives transactions from client systems or other Equifax systems (containing credit bureau data). The reported decisions are based on customer-specific criteria, which are enforced via configured rules within the InterConnect application, and consist of data such as demographics, credit data, and financial data.

The InterConnect application is run on Solaris UNIX servers and utilizes Oracle databases. The Equifax Technology and Analytical Services (TAS) – InterConnect Core Product team builds product functionality based on scheduled releases, typically two releases per year.

With respect to making modifications to InterConnect rules that determine reporting and processing output, user entities can elect to perform their own modifications or request that the Equifax TAS – InterConnect Core Product team perform the changes on their behalf. When an InterConnect rule is modified, a change notification is sent via e-mail that informs the user entity of the change. All InterConnect transactions are priced, taxed, and billed through CIS

Personal Solutions

The PSOL IT team, which is part of EIT, manages and maintains the Personal Solutions platform, consisting of the Personal Solutions application and Siebel Administration Console application. This eCommerce platform provides capabilities, such as enrollment of consumers, order management, and product delivery, via online and batch channels. Several credit related products are offered to consumers by various lines of business, such as US (direct and indirect marketing), U.K., and Fair and Accurate Credit Transactions Act (FACTA), using the Personal Solutions application and Siebel Administration Console application. Some of the products offered are Credit Watch, Tri Bureau monitoring, Score Watch, Credit Report, Tri Bureau Credit Report, ICO Score Power, and Adverse Action Disclosure. The Personal Solutions platform interacts with multiple credit card processing vendors to process credit card transactions to support customer payments for Personal Solutions services. These credit card transactions can occur both at the time of purchase and at periodic billing intervals based on the payment option selected by the consumer. The majority of consumers that purchase subscription products select the monthly recurring billing option but can also select annual or quarterly. The personal solutions batch billing process runs daily, charging consumers whose monthly, quarterly, or annual billing renewal falls on that date. The data processing and internal controls supported by these credit card processing vendors are excluded from the scope of this examination.

The Siebel Administration Console provides capabilities for the call centers to manage consumer profiles, orders, cancellations, and refunds. The platform is made up of several subsystems such as consumer registration, order management, product fulfillment engine, billing and payment services, print delivery subsystem, monitoring and alerts generation.

Consumers interact on-line via web interfaces either directly through EIS or indirectly through partner channels. The Personal Solutions application and Siebel Administration Console application are run on mid-range Solaris UNIX servers with Oracle databases.

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication

Control Environment

Organization

The Equifax internal control environment is designed to remain current and support the needs of Equifax customers with the central component of the control environment being local management. Local management has the responsibility of promoting awareness and monitoring compliance. The policies and standards of Equifax are communicated and are available through orientation and awareness programs.

The Equifax Board of Directors also influences the control environment. The Board of Directors consists of individuals who are independent from management, none of whom have any direct family or financial relationship with management. Equifax also has established an Audit Committee of the Board of Directors that meets regularly and reports to the Board of Directors on a quarterly basis.

Equifax Information Technology Organization

The EIT organization is led by the Chief Information Officer (CIO), who is responsible for global technology strategy, architecture, system development/maintenance, and operations. The CIO has the following direct reports, which represent a segregated and fully defined Information Technology organization:

- Eight Chief Information Officers who are each responsible for business sector and corporate support technology implementation
- Senior Vice Presidents of IT Strategy & Effectiveness, Enterprise Architecture, Platform Engineering, and Global Infrastructure Operations

Equifax maintains organizational charts that define segregated job responsibilities.

Within EIT, the IT Risk & Compliance team maintains an IT Risk Register and monitors specific IT operational risks. The IT Risk & Compliance team provides input into the annual risk assessment process and also tracks and reports on the remediation of IT risks.

Global Security

The Global Security organization is independent of EIT and reports to the General Counsel and Chief Legal Officer. Global Security is responsible for defining information security policies and standards and monitoring compliance with security policies and standards.

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication

IBM Global Technology Services - US

The maintenance and monitoring of some enterprise infrastructure and systems is outsourced to IBM Global Technology Services. EIS maintains exclusive ownership of the facilities and systems used to deliver enterprise applications, databases, and systems. IBM provides the technical resources and executes Equifax defined policies and procedures related to components of Systems Development and Maintenance, Logical Security, Job Scheduling and Problem Management, Network Performance Monitoring, and Backups. The IBM organization is structured as follows:

- Project Executive – responsible for executive relationship.
 - Solutions Management – responsible for creating statements of work for customer requests.
- Service Delivery Executive – responsible for managing overall service delivery and service level measurement, achievement, and reporting. IBM also has Availability Service Leads that coordinate with Operation teams to maintain service availability.
 - Operations Personnel – responsible for daily operations of the various technology segments through which Equifax delivers information products to their partners and clients. The technology segments include, but are not limited to Web Hosting, Network and Voice Infrastructure, Mainframe system support, Midrange system support, Security, Disaster Recovery, and Problem Management.
- Contracts & Negotiations – responsible for contract administration, negotiation, issue resolution, and compliance as well as interfacing with Equifax contract and legal personnel.
- Financial Analyst – responsible for financial planning, analysis, and reporting, as well as customer invoicing.

Personnel Policies and Procedures

Equifax applicants for employment are required to undergo multiple screenings as pre-employment qualification for work. Offers of employment made to new hire candidates are contingent upon the successful completion of the applicant screening processes and indisputable accuracy of statements and representations made throughout the hiring process. The following pre-screens are utilized as part of the new hire process:

- Verification of information on the application to include professional references and job history;
- Satisfactory background investigations that do not reveal felony convictions;
- Drug testing using the ten panel drug screen which identifies illegal drugs, controlled substances, doping agents, and pharmaceutical drugs; and
- Criminal and consumer credit checks.

The Human Resources (HR) department manages, documents, and updates the personnel policies and distributes the Equifax Business Ethics and Compliance Manual, “Leading with Integrity” to staff in its

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication

locations, in local languages, and customized for local regulations. The “Leading with Integrity” guide cover topics including but not limited to:

- Core Business Ethics
- Code of Conduct
- Human Resources Policy
- Substance Abuse Policy
- Political Participation
- Environmental Health and Safety
- Accounting Integrity and Internal Controls
- Fraud and Embezzlement
- Regulatory Practices & Requirements for Our Business
- Confidential Information and Intellectual Property
- Conflicts of Interest
- Relationships with Suppliers and Vendors

Once hired, new employees are required to review the Equifax Business Ethics and Compliance Manual and must sign an acknowledgement indicating they read the manual, are familiar with it, and agree to comply with the policies contained therein. A Quick Reference Guide is distributed on an annual basis to all U.S. employees, which lists the key elements of the Ethics and Compliance Program. A brief security awareness orientation is also provided upon hire and further references are provided to the Global Security Awareness intranet. The Global Security Awareness intranet site contains ten security awareness modules, additional documentation and awareness collateral. New employees are required to complete additional on-line awareness training and testing within 60 days of beginning employment. The results of this training are tracked by Security Compliance and reported to the Equifax senior leadership to increase the assurance that completion of the self-study coursework in a timely fashion.

Performance reviews are completed at least annually as part of the Performance Review process. Objectives and responsibilities are detailed at the beginning of the review process, company-wide mid-year reviews take place and performance is reviewed and graded at the end of the review process. The entire process is conducted for all employees during the same timeframes each year.

Additionally, Equifax maintains organizational charts to display the established reporting relationships, which provide managers with information regarding their responsibilities and authority. Equifax also maintains Sarbanes-Oxley Section 404 process documentation that captures key process and control knowledge.

Risk Assessment Process

Annually, Equifax business units complete strategic planning to address objectives, risks, and issues. An Enterprise Risk Management (ERM) program defines specific enterprise risk management goals and

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication

actions for each business area and monitors progress on the achievement of goals throughout the year. The ERM program is managed by the Chief Financial Officer. Within IT an IT Risk & Compliance function identifies, assesses and monitors specific IT risks as part of the overall ERM program.

In addition, Equifax's Internal Audit function includes selected high risk operations and projects in its annual plan. The results of these risk assessments are presented annually at Audit Committee meetings, which address the organization by risk area using a heat map methodology to illustrate risk impact.

Monitoring

Internal controls are tested by internal and external auditors as a part of Sarbanes-Oxley Section 404 compliance efforts, operational audits, and service auditor reviews. Equifax has an independent Internal Audit department that performs independent appraisals of certain Equifax business entities' internal control activities and operating procedures. Internal Audit is organizationally segregated from the implementation and execution of business controls to allow Internal Audit personnel to maintain objectivity over the area being reviewed.

Internal Audit reports on noted internal control findings and recommendations are distributed to and discussed with company management and the Internal Audit Committee or the Audit Committee of the Board of Directors on a regular basis. The presentation includes updates to the Audit Committee on Equifax's significant risk areas, the status of unresolved audit points, the results of periodic reviews, and staffing.

As part of the ERM program, Internal Audit leads an annual risk assessment process to identify and assess key risk areas across the business. The top risk areas are reviewed and monitored by Management periodically throughout the year. The ERM program is reviewed with the Board of Directors annually with periodic updates on specific risk areas.


An IT Risk & Compliance function exists within IT. This group maintains an IT Risk Register and monitors the mitigation and remediation of IT risks (including those identified through the ERM program). The IT Risk Register is reviewed periodically with the IT Leadership Team throughout the year.

Internal Audit also performs various annual audits covering information technology controls. In addition, Equifax engages a third party to perform annual penetration testing on its IT environment. Global Security also performs monthly security scans of the Equifax network.

Information and Communication

Employees are encouraged to communicate issues via the toll-free compliance hotline, maintained by an outside vendor, which allows for an anonymous communication. Additional avenues of communication include direct contact with the Compliance Officer in writing, via email, or via telephone. Employees can confidentially and anonymously report complaints regarding questionable accounting, internal controls, and auditing matters. The Audit Committee receives quarterly updates relating to compliance issues reported to Security Compliance and the Compliance Officer, including detailed reports for issues related to accounting and financial reporting matters.

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication



As described in the Control Environment section above, Equifax maintains and distributes the Equifax Business Ethics and Compliance Manual to employees to educate them regarding company security principles and policies. Ethics and Compliance policies and narratives are available via the corporate intranet and the company website.

IT Leadership develops annual IT long range and short range plans based on monthly meetings with the CEO and Executive Leadership team. The plans are used to set goals for the achievement of the Equifax business strategy and are communicated to technology managers. Programs and projects are adjusted throughout the year to achieve the goals in the IT long range and short range plans.

Description of General Computer Controls

Control Objective 1: Systems Development and Maintenance

Control Objective

Controls provide reasonable assurance that modifications to the production applications, databases, operating systems, and firewalls are authorized, tested, approved, properly implemented, and documented.

Description of Controls

General Change Control Process (ACRO, CIS, CDC, CCS, EMS Gateway, EMS Ops, InterConnect, and PSOL)

Equifax has a change management approach that allows for project initiation, tracking, resource assignment and checkpoints, as required. Internally initiated changes to application programs, with the exception of emergency fixes, are initiated with an Investment Navigator (INAV) work request. INAV is an automated tool that Equifax uses to implement its SDLC and methodology. INAV includes process workflow, information fields, and system embedded controls for project management, demand management, time management, resource management, financial management, and the dashboards and reporting to support the aforementioned functions. For the period of January 1, 2012 to May 29, 2012 the ManageNow change management tool was used. As of May 30, 2012, ManageNow was replaced by Maximo. ManageNow/Maximo is the HTML interface change management tool utilized by Equifax and IBM. The ManageNow/Maximo system contains the process workflow, information fields, approval fields, system embedded controls and all necessary support information as defined in the Equifax Change Management Policy and Procedures. Supporting information includes the change classifications, change risk definitions, implementation scheduling, back-out plans, contacts, test results, and descriptive information on how to execute changes.

There may be some scenarios relating to certain minor or emergency changes where the INAV tool is not utilized. In these scenarios, the major control points described below are still performed though the documentation may be less formal.

The typical change proposal types are categorized into three categories: customer new implementation, customer maintenance, and customer enhancement.

A Change Manager is defined in the context of this narrative as an individual responsible for tracking the completion of required tasks for a change to production from inception through implementation. The role of the Change Manager may be occupied by various management roles depending on the system and the phase in the change lifecycle.

Change Authorization

Changes to applications and programs, with the exception of emergency fixes, are initiated with a change request. Based on the complexity of the change, the analyst may also fill out a business and/or technical requirement document describing what is involved in the change, which is included with the change request form. The various system teams each have separate approaches for approving changes:

Description of General Computer Controls

- ACRO uses a Change Management Board.
- CIS has minimal changes, which are reviewed weekly in a Project Review Session. CIS participates in the weekly Global Infrastructure/IBM change control meeting. CMS uses a committee comprised of business and IT personnel that meet as needed to address open issues.
- Commercial Credit uses a Change Management Board that meets as needed to address open issues.
- CDC has a Change Management Board that meets as needed to address the pipeline and any open issues.
- EMS Gateway and EMS Ops use a tool (Mercury Quality Center) to communicate with the Change Manager.
- InterConnect creates a Proposal Request to manage the incoming Customer Fulfillment proposals. A Level 1 estimate is derived during the proposal phase. The Level 1 estimate is documented into a Project Statement/Work Order by Sales to Finance. Once the Proposal is approved and closed, it is converted to a Project Request.
- The PSOL Change Manager consults with the key resources in the Business, Finance, and IT prior to creating a change request in ManageNow/Maximo. If the change is a part of an official PSOL release, a subsequent iNav change is created.

Once a proposed change is requested and approved, the Change Manager enters the change as a project into the INAV system. Resources are assigned to the change as warranted by the change specifications. Resources are assigned based on individual skill sets (programming language, software, hardware) and availability. For ACRO, either the Developer or the Manager enters the change as a project or work request into the INAV system.

Management prioritizes approved changes based on criteria that may include the type of change, risk, impact, and/or implementation scheduling. The priority is included with the change in the INAV system.

Each request that is approved is controlled by INAV workflow. Some of the detailed workflow steps may vary depending on the impacted application(s).

Change Testing

While INAV is used to monitor the progress and approval of testing, the test requirements and tools used to document testing may vary depending on the impacted application(s). The Change Manager is responsible for determining whether a change requires unit, load, system, regression, and user acceptance testing and assigns required tasks to the appropriate groups. The following tools are utilized in addition to INAV for testing of changes:

- ACRO: Turnover Control Database (TOP) – Lotus Notes
- CIS: Customized System, Integration and Regression Test Environments, Staged Endeavor Change Deployment and Fulfillment System Product Testing.
- Commercial Credit: Mercury Quality Center, WinRunner and Quick Test Pro
- CDC: Mercury Quality Center
- EMS Gateway and EMS Ops: Mercury Quality Center
- InterConnect and PSOL: Mercury Quality Center, LoadRunner and Quick Test Pro

Once testing is complete, the test results are reviewed and the status is updated within INAV to indicate the completion of testing. User acceptance testing is performed for application-level changes, but not database-level changes. Once all testing is complete, the INAV ticket is updated with signoffs from the individuals completing testing.

Change Approval

Once the appropriate testing has been performed and signed off within the INAV ticket, the Change Manager documents the approval for the implementation of the changes into production within INAV.

In ACRO, once all of the appropriate testing has occurred, the tester signs off in TOP. The tester then accepts the change in ManageNow/Maximo. It is TOP and the ManageNow/Maximo signoff that determine approval to install. INAV signoff is completed after implementation.

The EIS and IBM teams utilize the ManageNow/Maximo tracking system to control the implementation process and document the required implementation approvals. Back-out plans are documented in ManageNow/Maximo to allow changes that are not successfully implemented to be rolled out of production.

Change Implementation

For InterConnect, the Configuration Management team is responsible for installing the releases. IBM uses ManageNow/Maximo to manage the implementation of changes, such as URL's, database, and webhost.

For all other systems, the implementation process is controlled through the ManageNow/Maximo system. Back-out plans are documented in the ManageNow/Maximo tickets to allow changes that are not successfully implemented to be rolled out of production. Endeavor is also used for the z/OS mainframe applications. Programs under the control of Endeavor are recompiled in a secured staging library where source/object code transitions from development to production. The staging library is secured to prevent programmers from altering source/object code in a QA stage. On implementation day, the program is moved to the production library. Changes to the midrange applications are moved to production through the use of scheduled jobs. All packages must be approved by authorized individuals prior to the move to production. The scheduled jobs are coded to only move approved packages into production. These changes are moved to production by authorized individuals who have been granted administrator access.

Change Documentation

Implemented changes are documented in ManageNow/Maximo. The lifecycle of the various system changes are documented within INAV. Each system also utilizes additional programs for documenting changes:

- For ACRO and CIS, the test source code libraries are controlled by Endeavor. A master checkout document is utilized to track what modules are currently being modified. Once a modified program has been turned over to production, it is removed from the master checkout document.
- EMS Gateway, EMS Ops, and PSOL utilize Quality Center as a change documentation repository for testing artifacts such as test cases and test results.
- CDC utilizes documents stored on a central file server to repose artifacts such as test cases and test results.

- InterConnect and Commercial Credit document the test results from the test execution tasks in INAV and also retains documentation within Mercury's Quality Center.

CMS Change Control

The Global Corporate Platforms IT group is responsible for completing system development and maintenance projects for the Oracle modules and custom programs used by Credit Marketing Services for project management and billing.

The Enterprise Financial Systems group maintains a service level agreement with TCS, a third-party organization that provides contract IT services, to perform CMS system development, quality assurance, and change management functions.

Different systems are utilized to track projects and changes. For the period of January 1, 2012 to August 20, 2012 the iStream change management tool was used. As of August 20, 2012, iStream was replaced with SharePoint. The iStream/SharePoint system is used for tracking changes. These systems do not allow a project to progress to the following step until the previous requirement is completed.

Change Authorization

Changes must have a change request form and database change request form completed and signed by the originator, Design Administrator, and the Database Administrator. Change requests are initiated by a user and logged on iStream/SharePoint and are sent to the business owner or IT owner who approves it, and is then prioritized.

An application log is maintained that logs requests that are reviewed, categorized based on project size, and approved by the responsible Development Manager prior to work initiation. Work requests must be approved by the Global Corporate Platforms IT Manager or appointed backup.

For medium-sized projects, design specifications are documented with signature approval. For medium-sized projects, user and system documentation is updated to reflect any changes to functionality. For large-sized projects, prior to migration to production, new programs must be approved by Global Security, Architecture, and the Development Manager as production ready, secure, and consistent with Equifax architecture.

For large-sized projects, detailed technical specifications must be created and approved with signatures for the Detail Design, Input and Output Specifications, Test Plan, Interface Specifications, Requirements, Application Controls, User Documentation, and Data Conversion Plan.

Change Testing

All changes and enhancements initiated by a business owner and IT require a formal test plan and approval by the Development/Support resource and Global Corporate Platforms IT management to be documented within iStream/Sharepoint (request System).

For medium and large projects, a written test plan must be created and executed. For these projects, the test plan and test specification sheet must include the request originator's signature to indicate approval of completed tests. A test specification sheet is completed and signed by the Originator, Designer Administrator, and Database Administrator.

For small and medium projects, the Development Manager must sign off after the successful completion of Unit and System tests. For medium and large projects, user acceptance testing must be completed with customer signoff of the test results.

Change Approval

Code cannot be migrated to production without appropriate authorization. Changes must be approved by the IT Manager prior to moving into production. Once approved by the IT Manager, the change can only be scheduled/released for production implementation by the Global Corporate Platforms Database Administrator.

Change Implementation

For small, medium, and large projects, a back-out plan must be documented and approved prior to the initiation of the testing phase. For projects, back-out procedures are documented within the test plan for the project. Programs are restored from the daily CMS backup in the event of an implementation issue. Once the code has finished the User Acceptance Testing phase, it is assigned to an Enterprise Financial Systems Database Analyst who manually implements the code into production. Only authorized personnel can perform production program implementations. Developer access to the production environment is restricted to read only.

Change Documentation

All work requests are logged, reviewed, prioritized, and approved within iStream/Sharepoint or INAV. Testing documentation is stored on a network drive.

For small, medium, and large projects, periodic user reviews are conducted and communicated via status reports, update meetings, and/or documented meeting minutes.

Operating Systems Changes

For Mainframe environment, zOS operating system changes are provided by IBM for implementation into the Equifax systems. The zOS Operating System Software is installed first on a test LPAR used by IBM/ Equifax Software teams for "testing" and identifying software issues before rollout to production environments.

After testing on the test LPAR, the Operating System is migrated to all production LPARs. There are scheduled maintenance windows agreed upon with Equifax Business Units as their particular LPARs are to be upgraded. This process will provide a duration for testing by the business units during which time they perform, production scripts which simulate production within the new Operating System environment. After several tests are performed over several weekends, a target date is selected for production implementation.

The change management process is used (ManageNow/Maximo) to open change tickets for implementation during designated testing windows. These change ticket requires approvals from respective business units and IT Operations.

Mainframe Security/Integrity APARs are released by IBM and are classified High, Medium or Low risk. APARs are applied using the change management process and within the recommended time line. A

change is submitted by the support teams via the normal change management tool (ManageNow/Maximo) and rolled out within the normal Initial Program Load (IPL) windows published in the Equifax Technical Calendar. Once IPL is complete, checkout by technical teams will occur to verify that there are no issues or concerns with implementation.

For the midrange environment, Change Request tickets are opened in the ManageNow/Maximo tool for both operating systems upgrades and operating system security patches. These are normally created up to two weeks in advance but expedited changes can be made for critical security issues. All of the business unit teams that are impacted by the operating system change review and approve the change request before it is scheduled. Operating system changes are made to one zone for testing and validation, while production load is moved to the alternate zone. After the change is made, System Administrators test and validate the updated operating system, while application teams validate the application platforms are working properly. Once validated the operating system change is then made to the alternate zone, and the production load is returned to the normal dual-zone architecture. The ticket is then closed after updating the documentation as necessary.

Firewall Change Control

The IBM firewall group manages the operations and change procedures for the firewalls that protect Equifax systems for the period 1/1/12-6/30/12. For the period 7/1/12 to 10/31/12, Equifax Global Infrastructure Operations managed the operations and change procedures for the firewalls that protect Equifax systems.

The requesting group initiates a firewall change by creating a ticket in the ManageNow/Maximo system. The ticket is assigned to the IBM firewall group/Equifax Network Operations team who reviews the request to determine whether a firewall rule already exists that would pertain to the request. If a new rule is required, then the change is identified and scheduled for the maintenance window.

Changes must be approved by appropriate Equifax and IBM personnel, which is documented on the ManageNow/Maximo ticket. The ability to implement firewall changes into production is limited to authorized personnel.

Once the change is implemented, the requestor is notified and performs end-user testing to determine appropriate functionality. If the end-user test fails, a problem ticket is opened with IBM/Equifax Network Operations for resolution. Global Security conducts periodic reviews of firewall rules to ensure they continue to meet security standards.

Control Objective 2: Data Center Physical Security

Control Objective

Controls provide reasonable assurance that physical access to the computer equipment and storage media is restricted to appropriately authorized personnel.

Description of Controls

Data Center Physical Security Protections

EIS facilities are protected by multiple layers of physical security controls with more restricted access areas covered by the highest level of protections. Restricted access areas include areas where equipment, data, storage, media, and documentation are kept. The following physical access controls are in place for the Alpharetta, Georgia data center:

- Proximity badge reader systems;
- Closed circuit television (CCTV) video cameras;
- Door alarms;
- Biometric devices;
- Security guards, posted and roving on-site on a 24 hours a day, 7 days a week; and;
- Sign-in/Sign-out Log Sheets.

Data center entrance points require a valid proximity badge and matching biometrics authentication via hand or fingerprint scan. A man trap door configuration is installed at the data center entrance points. For mantrap door operations, the first door must be secured before the second door lock can be activated.

Visitor Sign-In logs are maintained for data center visitors and require the sign-off of a data center cleared escort. In addition, the Global Security team performs one annual review of physical access to the two data center rooms.

Facilities Physical Access Authorization

Requests for access to the Equifax data center are administered through an electronic workflow. Requests submitted via the electronic workflow provide an audit trail of approvals with timestamps, and require manager approval before allowing the provisioning of the account or the access privileges. Once the request is approved, the user access is added to the security system by Allied Barton security personnel. Allied Barton meets with the new users to register their fingerprint for the biometric readers. Access card reader is administered through the DSX. Refer to control objective 3, "Logical Security," for details on the removal of physical access.

Data Center Access

Authorized access to the Alpharetta, Georgia data center is granted to personnel with a justified business need, and includes the following:

- Operations Personnel;
- Security Team Personnel;
- Building Facilities Personnel; and

- **Facilities and Maintenance.**

Access logs are maintained for the proximity badge reader activity. Badges which have not been used in 60 days are automatically deactivated. New access to the data center must be submitted using an electronic workflow. The requestor's manager and data custodian for the restricted area must approve the data center access form.

Security Guards

Security guards are posted 24 hours per day, 7 days per week at various entrances and exits. Between 6:00 AM and 8:00 PM on weekdays, Equifax employees entering a building must scan their badge at the entry gates in order to pass the security desk. Visitors must be signed-in by an Equifax employee or contractor, present photo identification, and are given a visitor's access badge. If a visitor does not have photo identification or is present for an interview, they are escorted by an Equifax employee.

Security officers are posted 24 hours per day, 7 days per week within the data center. The security officers located at Alpharetta data center respond to emergency exit alarms for restricted areas.

Security Cameras

Over 50 digital and analog cameras are positioned throughout the Alpharetta location, including parking lots and parking decks. Video is monitored from the two security operations centers locations in Building 1 and Building 2. On-duty guards are responsible for reviewing the monitors for suspicious activities. Cameras are placed at perimeter entrances and exits, and entrances to restricted areas. Each digital camera receives a live feed and stores the recorded video on hard drives in a secure room.

Control Objective 3: Logical Security

Control Objective

Controls provide reasonable assurance that logical access to programs and data for the ACRO, CIS, CMS, CCS, CDC, EMS Gateway, EMS Ops, InterConnect and PSOL applications, operating systems, and databases is restricted to properly authorized individuals.

Description of Controls

Roles and Responsibilities

Equifax's implementation of logical access control relies upon dedicated security and compliance teams for continuous oversight of logical access, technical system security controls, and process controls for the proper authorization of access to networks, operating systems, databases, and applications. The following organizations and personnel are involved in the policy, administration, and management of logical security:

Organizational/Personnel	Role/Responsibility for Access Management
Equifax IT Risk & Compliance Team	Provides the policy and oversight of information technology security for logical access management activities.
Equifax Global Security	Defines and maintains Global Security Policies and Standards for all aspects of information and physical security. Monitors compliance with security policies and standards.
Equifax Personnel Managers in Business Units	Act as first level approvers of logical access requests by verifying business need.
Equifax Data Custodians in IT	Act as second level approvers of logical access to data sets on a "least privilege," "need to know" basis. In some cases, the user's manager may be the same as the data custodian. In these situations, the request is escalated to the manager's manager for approval.
Equifax Access Management Team	Manages centralized access provisioning and de-provisioning for audit relevant systems. Provides daily oversight of access request workflow tools, authorization requests, and entitlement reviews. Facilitates the review of user ID lists to justify continued business need for logical access. Provides communication and status of terminations.
Equifax Mainframe Security Team	Administers security to the mainframe operating system and select application systems
IBM Global Technology Services	Administer security of certain UNIX operating systems.
Equifax Database Administration Team	Administer security of database platforms.

Description of General Computer Controls

Organizational/Personnel	Role/Responsibility for Access Management
Equifax HR	Provides the authoritative source for personnel status and management team assignments as a means of verification for logical access processes. Provides communication and status of terminations.
IBM Firewall Security Administration/Equifax Network Operations	Administers changes to the firewalls protecting Equifax systems. IBM responsible for period 1/1/12-6/30/12. Equifax Network Operations responsible for 7/1/12-10/31/12.
Equifax Application Security Administrators	Administers role based security privileges within select applications delivered to internal and external clients.

Password Controls

The Global Security Policies and Standards apply to the network, operating system, database, and application layers of the technology architecture. The policies and standards covers multiple password and password management topics, including password minimum length, forced password expirations, and password history.

Authorization

Logical access requests for new accounts and modification to access privileges must be submitted using an electronic workflow through IDM – Identity Manager. Requests submitted using the electronic workflow approval provide an audit trail of approvals with timestamps. Privileged access is granted in the same manner but is restricted to authorized individuals who provide system administration support.

One or two levels of approval are required for access requests. The number of required approvals depends on the type of access being requested. Individuals requesting access to privileged data are required to have two levels of approval with the additional approval provided by the data custodian. Those approval levels are the requestor's manager and data custodian.

Review of Logical Access

Equifax performs entitlement reviews that analyze the appropriateness of logical access granted to each user. Logical access entitlement reviews are applied to Equifax databases, operating systems, and applications on a periodic basis.

The entitlement review process requires authorized individuals to review the user accounts on a given system for compliance with the Global Security Policy and Enterprise Identity and Access Management (EIAM) Standards.

Equifax is in the process migrating the current manual, custodian only access reviews to an enhanced access certification through automation (Equifax Access Manager tool) and an additional layer of certification by managers. During this migration period, access reviews will be performed using one of the following methods:

1. Manual Certifications

2. Automated Certifications using Equifax Access Manager tool

Manual Certification:

There are four phases for this process: (1) information gathering and distribution, (2) certification of user accounts, (3) remediation of defects; and (4) validation of remediation activities.

During information gathering and distribution, business units will gather current user lists for the systems in scope for the entitlement review. The user list contains the following data, where technically possible, for each user account on the system:

- UserID – The Account ID on the system
- User Name and Employee ID – The first and last name and Employee ID of the user
- Account Create Date – The date the account was created on the system
- Account Last Login Date – The last date the account was used
- Current Account Status – Active, Inactive, Disabled, Locked, etc.
- Account Privileges – The specific functional privileges available to the account

Business units gather the user lists from the appropriate source for each system. This source may be an automated list through IDM, the system administrator, or, in some instances, the custodian. Once the user list information has been gathered for the relevant systems, it is distributed by the business unit to the reviewers (custodians and/or managers) for validation.

Once the reviewer has completed the entitlement review for all user accounts in the system and annotated the user list, the annotated user list is returned to the Access Management Team.

If instances of inappropriate access are detected during the entitlement review, the business unit is responsible for the submission of the appropriate request to the system/account administrator or workflow to execute the action (delete, disable, modify access) specified by the reviewer.

Once the system administrator indicates completion of the specified action, the business unit gathers a new user list for the system to confirm that the specified action has been completed for each user account. If any defects are identified, the Access Management Team will work with the business unit and system administrator until the defect is resolved and a clean user list is obtained.

Automated Certification:

There are two phases per certification cycle (quarter) using the Equifax Access Manager tool:

- Manager Campaign phase
- Custodian Campaign phase – Custodian could be an application owner or an Entitlement Owner

Each phase, run sequentially (manager campaign followed by a custodian campaign), goes through following five steps:

- Information gathering / data aggregations
- Certification Generation by compliance team

- Access certification (review) by owner
- Access Remediation by revocation teams/tools
- Remediation confirmation (closed loop remediation)

The certification of user accounts requires the reviewer to consider each user account and validate the following:

- The user still requires system access to fulfill their job responsibilities.
- The access level granted to the user is the least privilege necessary for the user to fulfill their job responsibilities.

The reviewer determines the appropriateness of access privileges and selects the appropriate action in the tool: Allow, Revoke, Modify. Delegations (items that the reviewer forwarded to an additional party for additional review) are returned to the reviewer for final review and sign off. Revoke actions result in manual or automated removal of access. Entitlement review actions only allow for the reduction of access. Any new or increased access required is requested through the Access Request process.

Termination of System Access

Equifax manages the termination of system and facility access through the use of HR notifications and management requests for the removal of access. Upon receipt of a request for the termination of access from either HR or an EIS manager, the Equifax Access Management team executes the following actions:

- Notification to application security administrators to terminate or disable access;
- Notification to physical security administrator to terminate or disable access;
- Performs the removal of access or disables access for selected applications;
- Performs follow-up to help increase the assurance that termination actions are completed; and
- Maintains records of the above actions and notifications.

Terminations are communicated from HR to the Equifax Access Management team through the delivery of a daily termination reports from Equifax's HR information system. Equifax's Identity Management System immediately terminates access to the Equifax network by systematically disabling accounts through a direct connection to the Active Directory system.

In addition, an annual reconciliation between all badge holders with access to Equifax buildings and an HR listing of active employees, contractors, and contingent workers is completed. Any discrepancies are researched and corrected in a timely manner.

IQNavigator is the tool used to manage contractor and contingent worker status at Equifax. On an annual basis, a reconciliation between IQNavigator and an HR listing of active employees, contractors, and contingent workers within the HR information system is completed to determine that contractor and contingent worker status is accurate both in IQNavigator and the HR information system. Any discrepancies are researched and corrected in a timely manner.

Internet Facing Servers

For details on internet facing servers, please refer to the Network Performance Monitoring section within Control Objective 5.

Control Objective 4: Job Scheduling and Problem Management

Control Objective

Controls provide reasonable assurance that processing is scheduled appropriately and deviations are identified and resolved in a timely manner.

Description of Controls

Job Scheduling Technology

On the mainframe, the IBM CA7 utility is used for job scheduling and execution. The IBM CA11 utility is used to restart jobs that have failed to complete. Various tools are used to schedule and monitor jobs that are on the midrange environment.

Job Scheduling Changes

Equifax job scheduling changes are tracked and managed. The IBM Global Technology Services Operations Center Supervisor and his staff receive email alerts notifying them of pending changes for the current job schedule that are on the mainframe environment. Change requests for both mainframe and midrange environments must receive approvals from Equifax and/or IBM personnel prior to being implemented into production. Changes to job scheduling are tested to determine that the changes were made as requested. Evidence of testing approval is retained.

If problems arise with the implementation of job schedule changes, a trouble ticket is created in and assigned to an Equifax or IBM Operator by job function and area. The Equifax or IBM Operator is responsible for closing the open tickets. If an issue cannot be resolved in a timely manner, based on the set severity level, the Operator escalates the item to the duty Supervisor who handles the request with the appropriate resources.

Job Monitoring

IBM uses CA7 utility for job scheduling and CA11 utility for job restarts. The operator logs into CA7 and checks for jobs which need to be restarted and job amendments by selecting each job in the available queues. CA7 shows the operator where the job failed and provides information needed to help the operator restart the job. Jobs are tracked with these systems and at anytime a job queue can be displayed to show pending requests and their status. If restarting the job does not correct the issue, an incident is logged and resolved through the problem management process described below.

Problem Management Process

The Problem Management process is managed through the IBM Help Desk. Equifax employees can submit a problem management ticket through the online ManageNow/Maximo system or call the Level 1 Help Desk. Once an incident call or problem ticket is received by the IBM Help Desk, the incident is determined to be a new or existing problem. If it is an existing incident, then the record is reviewed by the Level 1 Help Desk to determine if the incident was already resolved, which is confirmed with the end user. If the incident has not been resolved, the appropriate work group is assigned.

If it is a new incident, a problem record is opened and the Help Desk associate determines if the problem can be fixed immediately or if it needs to be assigned to a Level 2 or 3 support workgroup. The assigned workgroup resolves the problem and updates the record. ManageNow/Maximo is used to document this process and resolution. The information documented in the ticket includes, but is not limited to:

- Customer information
- Date and time the problem was identified
- Date and time the problem was reported, including a symptom description and type of problem
- Failing resource/component
- Actions taken to resolve the problem, including date and time action was taken
- Analysis of initial information to determine appropriate problem record assignment

The end user is updated on the status via email or phone. If necessary, a Root Cause Analysis is performed as described below. If the resolution is determined to be a permanent fix or a change is required, then the change management process is initiated. If not, the record is updated and closed.

Root Cause Analysis (RCA)

The Root Cause Analysis (RCA) is a procedure to identify, document and implement a solution to resolve the true cause of a problem, as opposed to resolving only the symptoms of the problem. The symptoms may be alleviated when service is restored, but further action (i.e. a permanent fix) may be required to address the root cause.

The type of RCA (formal or informal) is based on the severity level of the problem, with 1 being the highest severity. Severity level 1 or severity level 2 problems require a formal technical RCA. Severity level 3 problems are assessed on a case-by-case basis to determine if an “informal” technical RCA should be performed. Severity level 4 problems do not require a RCA.

The IBM Service Delivery Team is responsible to coordinate completion for each formal RCA for platforms supported by IBM.

IBM works directly with the EIS application teams and with outside third parties when necessary to produce an RCA. If IBM is not responsible for problem resolution, then the problem resolution actor (whether an EIS internal team or an outside third-party) provides IBM with the technical RCA input within the required time based on severity level, using the RCA standards, after service is restored.

Problem Management Meeting

Incident Review/RCA meetings are held daily to review major problems including high-risk change implementations that failed in the production environment within the past 24 hours. If major problems occur after the Friday meeting and/or over the weekend, these problems are reviewed at the Monday morning meeting. The main objectives of the meetings are to review and manage open problems, RCA action items, identify open issues for escalation, and review problems more than 72 business hours old. The IBM Regional Delivery Service Manager, IBM local technical management, and EIS local and global operations managers are the primary attendees for this meeting.

Control Objective 5: Network Performance & System Capacity Monitoring

Control Objective

Controls provide reasonable assurance that network performance and system capacity are measured and monitored.

Description of Controls

The IBM Network Monitoring Center is responsible for monitoring network performance for the in-scope applications. The Transaction Monitor (T-Mon), Netview, Server Resource Management, and Omega Mon consoles are monitored throughout the day to identify process and batch run performance issues, CPU and memory utilization issues, failed system connections, backup performance issues.

IBM prepares a report of network performance trends that is shared at monthly meetings between IBM and Equifax. The report includes analysis of performance measurement metrics and root cause analyses for major outages occurring during the month.

System and Network Utilization is monitored and capacity and trending reports are generated on a quarterly basis and reviewed by Equifax. To compile the quarterly capacity reports, IBM generates capacity trending reports for ACRO Online processing, MIPS utilization for CMS, and CIS batch processing.

Internet facing servers are positioned within screened subnets and are protected via stateful packet inspection firewalls. Firewalls are configured to block all traffic that is not explicitly allowed in the firewall configurations. Refer to Control Objective 1 for a description of controls over changes made to firewalls applicable to the in-scope applications. Global Security also performs monthly security scans of the Equifax network.

Equifax also contracts with a third-party to execute network penetration testing at least annually. Network penetration testing is performed to search for security gaps in system configurations as a measure to prevent unauthorized and inappropriate access to Equifax systems and resources. Detailed results and potential fixes are distributed to administration and information security personnel who use the results to patch potential security gaps.

Control Objective 6: Backups

Control Objective

Controls provide reasonable assurance that programs and data files are backed up and rotated offsite.

Description of Controls

Daily full volume backups are executed for certain critical resources. Daily incremental volume backups occur for non-critical resources. Full volume backups are performed for mainframe production files every weekend with certain exceptions as identified and approved by the application owners. Refer to control objective 4 for further detail on the processing of backup jobs and procedures for resolving backup failures. Backup processes have been implemented and backup procedures are formally documented.

Description of General Computer Controls

For Mainframe applications, IBM DASD Storage team uses the IBM Removable Media Manager (RMM) system to maintain information about the status, content, and location of tapes by volume and serial number. The mainframe systems maintain a shared system catalog, which indicates where datasets are stored on disk drives.

Servers in the midrange environment are backed-up using NetBackup application.

For mainframe applications, IBM uses CA7 to schedule Disaster Recovery backups and HSM to create onsite backups. The DFRMM Tape Management tool is used to maintain information about the status, dataset name, and location of tapes.

z/OS global Mirror (XRC) housed in Equifax Disaster Recovery Site provides for a redundant copy of the Alpharetta data center volumes. Alpharetta production data is mirrored to the Equifax Disaster Recovery Site.

Two TS7720 Virtual Tape Storage (VTS) devices at the Equifax Disaster Recovery site function as the vault for all Equifax mainframe storage data and recovery.

Through the use of -Advanced Policy Management- and updated System Managed Storage (SMS) rule changes under Data Facility System Managed Storage (DFSMS), Equifax data is filtered by High Level Qualifier (HLQ) and rules are used to determine what data is backed up to the Storage Grid and into Equifax Disaster Recovery Site.

Servers in the midrange environment are replicated over the network to the Equifax Disaster Recovery Site.

Periodically test restores are conducted for a sample of critical data to verify the integrity of the data backup processes.

Complementary User Entity Controls

Equifax's and IBM's processing of transactions and the controls over the processing were designed with the assumption that certain controls would be placed in operation at user entities. This section describes some of the controls that should be in operation at user entities to complement the controls in place at Equifax and IBM. User entities' auditors should determine whether they have established controls to:

- Understand the distribution of responsibilities between user entities and Equifax, as set forth in user entities' contract with Equifax, and implement appropriate controls to determine that user entities' responsibilities are effectively performed to minimize risks.
- Develop and maintain adequate business resumption plans and/or provision sufficient insurance coverage to minimize the impact of potential disruptions to data processing activities or on-line access provided by Equifax.
- Maintain adequate safeguards that restrict physical access to computer terminals and printer output areas to only appropriately authorized personnel.
- Determine that employees are adequately trained to use Equifax applications.
- Determine that data transmitted to Equifax is accurate and complete.
- Implement and enforce effective information security policies and procedures.
- Change or closely monitor the default, initial passwords associated with the user IDs assigned to the organization.
- Request user access to application functions that promote adequate segregation of responsibilities and should grant access on a business-need only basis.
- User access capabilities and access to sensitive application functions be subject to periodic review for appropriateness. Procedures also should exist to promptly remove access capabilities for terminated and transferred employees.
- Restrict the user entity employee access to the Automated Credit Reporting Online, Commercial Credit, EMS Gateway, EMS Ops, and InterConnect applications based on job responsibilities.
- Develop and maintain standards, procedures, and controls for using Automated Credit Reporting Online, Commercial Credit, EMS Gateway, EMS Ops, and InterConnect applications to determine that each application is used in accordance with management's control objectives.
- Maintain a change management process with respect to modifying InterConnect rules.
- Review InterConnect change notifications to determine if InterConnect rule changes made by Equifax were appropriately authorized and approved.

The list of user entity control considerations presented above is not a comprehensive list of all controls that should be employed by user entities. Other controls may be required at user entities.

Section IV
Equifax's Control Objectives and Related
Controls and KPMG LLP's Tests of Controls
and Results of Tests

Use of Internal Audit

Throughout the examination period, members of Equifax's Internal Audit function performed some tests of controls for each of the control objectives. Members of the Internal Audit function observed the control being performed, inspected documentation and/or re-performed the control activities. When the work of Internal Audit was utilized, KPMG tested the work through a combination of independent testing and re-performance. KPMG also evaluated the competence and objectivity of the Equifax Internal Audit organization.

Equifax's Control Objectives and Related Controls and KPMG LLP's Tests of Controls and Results of Tests

Control Objective 1

Controls provide reasonable assurance that modifications to the production applications, databases, operating systems, and firewalls are authorized, tested, approved, properly implemented, and documented.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
1.01	Requests for changes to production applications, databases, operating systems, and firewalls must be authorized.	<p>Inquired of management and was informed that requests for changes to production applications, databases, operating systems, and firewalls must be authorized.</p> <p>For a selection of changes to the production applications, databases, operating systems, and firewalls, inspected change documentation and determined that changes were authorized based on the established workflows prior to development.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
1.02	For changes to production applications, databases, operating systems, and firewalls, testing is completed and signed off by the respective stakeholders.	<p>Inquired of management and was informed that for changes to production applications, databases, operating systems, and firewalls user acceptance testing is completed and signed off by the respective stakeholders.</p> <p>For a selection of changes to the production applications, databases, operating systems, and firewalls, inspected supporting documentation and determined that testing was performed and testing was documented.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

Equifax's Control Objectives and Related Controls and KPMG LLP's Tests of Controls and Results of Tests

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
1.03	Changes to production applications, databases, operating systems, and firewalls must be approved by authorized personnel prior to implementation into production.	<p>Inquired of management and was informed that changes to production applications, databases, operating systems, and firewalls must be approved by authorized personnel prior to implementation into production.</p> <p>For a selection of changes to the production applications, databases, operating systems, and firewalls, inspected supporting documentation and determined that changes were approved by authorized personnel prior to implementation into production, and that changes were closed and documentation was completed.</p> <p>For the same selection of changes described above, inspected the supporting documentation and determined that implementation instructions and roll-back plans were included and that there was evidence that the change activity was properly implemented.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
1.04	Access to implement production application, database, operating systems and firewall changes is limited to authorized personnel based on assigned job responsibilities. Access controls systematically enforce segregation of duties between program development and program implementation.	<p>Inquired of management and was informed that access to implement production application, database, operating systems, and firewall changes is limited to authorized personnel based on assigned job responsibilities with access systematically enforcing segregation of duties between program development and program implementation.</p> <p>For the ACRO and CIS applications, inspected the Endeavor system configurations and determined that access to implement production changes was restricted to only those users who require it to perform their job requirements and that users with program development responsibilities were restricted from making production changes.</p> <p>For a selection of servers supporting the CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, inspected system access reports of individuals with access to implement production changes and determined that access was restricted to only those users who require it to perform their job requirements and that users with program development responsibilities did not have system implement program changes.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><u>Results</u></p> <p>Controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 1 are operating with sufficient effectiveness to achieve this control objective.

Equifax's Control Objectives and Related Controls and KPMG LLP's Tests of Controls and Results of Tests

Control Objective 2

Controls provide reasonable assurance that physical access to the computer equipment and storage media is restricted to appropriately authorized personnel.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
2.01	Monitored security cameras monitor sensitive areas of the Equifax data center as well as the data center entrances and exits.	<p>Inquired of Equifax personnel and was informed that monitored security cameras monitor sensitive areas of the Equifax data center as well as the data center entrances and exits.</p> <p>Observed the Alpharetta, Georgia data center and noted that security cameras were positioned throughout the data center.</p> <p>Observed the Alpharetta, Georgia data center security personnel and noted that security personnel monitored the security camera activity.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.02	Access to Equifax's data center is restricted through the use of card-swipe access and biometric devices.	<p>Inquired of Equifax personnel and was informed that access to Equifax's data center is restricted through the use of card-swipe access and biometric devices</p> <p>Observed the Alpharetta, Georgia data center and noted that card-swipe mechanisms and biometric devices were used to secure the data center.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
2.03	Data center doors are protected by an alarm system.	<p>Inquired of Equifax personnel and was informed that data center doors are protected by an alarm system.</p> <p>Observed the Alpharetta, Georgia data center and noted that data center doors were alarmed.</p> <p>Observed an alarm test and noted that security personnel responded.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
2.04	Physical access to the Equifax data center must be approved by the user's manager and data custodian.	Inquired of Equifax personnel and was informed that physical access to the Equifax data center must be approved by the user's manager and data custodian For a selection of new users granted access to the Alpharetta, Georgia data center, inspected access request forms and determined that access was authorized by the application manager and/or data custodian and that access was appropriate based on job title.	No relevant exceptions noted. Exceptions noted, see below
<p><i>Exception</i></p> <p>One from a population of nine new users granted access to the Equifax Data Center did not have evidence of approval by the user's manager and data custodian.</p> <p>Management Response: <i>The exception related to a security guard who required access as part of his job role. Additional procedures have been implemented to ensure that all security guard data center access has documented approval of the manager and data center custodian.</i></p>			
2.05	Physical access to computer equipment and storage media is removed as employees are terminated.	Inquired of Equifax personnel and was informed that physical access to computer equipment and storage media is removed as employees are terminated. For a selection of terminated users, inspected facility access reports to and determined that access to Equifax facilities was removed.	No relevant exceptions noted. Exceptions noted, see below
<p><i>Exception</i></p> <p>One from a population of 2188 terminations was identified with an active badge to access Atlanta facilities.</p> <p>Management Response: <i>The exception was caused by an incorrect contract end date being entered in the contractor system. The badge access has been removed. An annual reconciliation of active contractors against the HR information system (which is the authoritative source for the identity management system) has been implemented (refer Control 2.06b).</i></p>			

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
2.06a	Equifax reviews data center access rights on an annual basis to validate ongoing appropriateness. Inappropriate access is removed.	<p>Inquired of Equifax personnel regarding Alpharetta, Georgia data center access monitoring and was informed that data center access was reviewed on an annual basis.</p> <p>Inspected the Alpharetta, Georgia data center access review and determined that it was performed and that access was removed and/or updated as necessary.</p>	Exceptions noted, see below
<p><i>Exception</i></p> <p>Four users identified to have badge access removed as part of the annual Entitlement Review were not revoked timely. Management re-performed the annual control as of 10/31/2012 and all users designated for removal were removed timely.</p> <p>Management Response: <i>Three of the four users were contractors who retained certain data center access but had no general building access (which is required to reach the data center) after termination. The access for all four users has been removed. In addition, management re-performed the annual entitlement review and confirmed that all users designated for removal were removed timely (refer Control 2.06b).</i></p>			
2.06b	An annual reconciliation between all badge holders with access to Equifax buildings and an HR listing of active employees, contractors, and contingent workers is completed. Any discrepancies are researched and corrected in a timely manner.	<p>Inquired of management and was informed that reconciliation between all badge holders with access to Equifax buildings and an HR listing of active employees, contractors, and contingent workers is performed annually.</p> <p>Inspected the supporting documents and determined that the reconciliation between all badge holders with access to Equifax buildings and an HR listing of active employees, contractors, and contingent workers was performed and documented.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
2.07	Visitors to the Equifax data center must be signed in and are escorted by an Equifax employee or permanent contractor during the data center visit.	<p>Inquired of IBM personnel and was informed that visitors to the Equifax data center must be signed in and are escorted by an Equifax employee or permanent contractor during the data center visit.</p> <p>Inspected the visitor's sign-in log and determined that an employee or permanent contractor had signed in visitors.</p> <p>Observed the visitation and escort process and noted that visitors are escorted by an Equifax employee or permanent contractor during visit to the data center.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><u>Results</u></p> <p>Except as noted above, controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 2 are operating with sufficient effectiveness to achieve this control objective.

Control Objective 3

Controls provide reasonable assurance that logical access to programs and data for the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, Interconnect, and Personal Solutions applications, operating systems, and databases is restricted to properly authorized individuals.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
3.01	<p>Application, operating system, and database password attributes are established as follows:</p> <ul style="list-style-type: none"> at least 8 characters in length. require changing every 90 days 7 passwords are remembered to prevent reuse 	<p>Inquired of management and was informed that application, operating system, and database password attributes are established.</p> <p>Inspected the ACRO, CIS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions application, operating system and database security settings and determined that:</p> <ul style="list-style-type: none"> passwords were configured to be at least 8 characters in length, password changes were systematically enforced at least every 90 days, password history controls were configured to prevent re-use of the 7 previously used passwords 	Exceptions noted, see below

Exception

1-The Commercial Credit application was not configured to enforce password history. This issue was remediated on 09/05/2012

Management Response: *The exception above has been remediated.*

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
3.02	Equifax user access must be authorized prior to granting the requested access.	<p>Inquired of management and was informed that Equifax user access must be authorized prior to granting the requested access.</p> <p>For a selection of users granted access to the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, operating systems, and databases, inspected the user access requests and determined that the request was authorized prior to granting access.</p> <p>For a selection of users granted access to the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, operating systems, and databases, inspected the assigned system access level and determined that the assigned access reflected the approved level of access, and that the access assignment was appropriate based on the user's job responsibilities.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
3.03a	Access for terminated Equifax users is removed in a timely manner.	<p>Inquired of management and was informed that access for terminated users is removed in a timely manner.</p> <p>Inspected the active user listings for the ACRO, CIS, applications, operating systems, and databases against the HR Terminations list to determine whether no terminated users retained enabled access to production applications, operating systems, and databases.</p> <p>Inspected the active user listings for the CMS, CDC, InterConnect, Commercial Credit, Personal Solutions, EMS Ops, and EMS Gateway applications against the</p>	<p>No relevant exceptions noted.</p> <p>Exceptions noted, see below</p> <p>Exceptions noted, see below</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
		<p>HR Terminations list to determine whether no terminated users retained enabled access to production applications.</p> <p>For a selection of servers and databases, inspected the active user listings for the CMS, CDC, InterConnect, Commercial Credit, Personal Solutions, EMS Ops, and EMS Gateway operating systems, and databases against the HR Terminations list to determine whether no terminated users retained enabled access to production operating systems, and databases.</p>	<p>Exceptions noted, see below</p>

Exception

- 1 Five from a population of 2188 terminations were identified with enabled accounts in ACRO.
- 2 Two terminated users from a population of 2188 terminations were identified with enabled accounts on the CMS Oracle Server.
- 3 One terminated user from a population of 2188 terminations was identified with an enabled account on the following servers: EMS Gateway, Commercial, PSOL Seibel, CMS and CDC.
- 4 Two terminated users from a population of 2188 terminations were identified with enabled accounts on three of four sampled servers for the InterConnect application.
- 5 Nine terminated users from a population of 2188 terminations were identified with enabled accounts in PSOL Siebel.
- 6 Two terminated users from a population of 2188 terminations were identified with enabled accounts in the CMS application.
- 7 Two terminated users from a population of 2188 terminations were identified with enabled accounts in CDC.
- 8 One terminated user from a population of 2188 terminations was identified with an enabled account in Active Directory. The Active Directory population of enabled accounts was 7,339.

Management Response: *The exceptions noted primarily relate to contractors and contingent workers. Management has implemented an additional control to annually reconcile the list of active contract/contingent workers against the HR information system (which is the authoritative*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
<p><i>source for active users) – see Control 3.03b. Subsequent quarterly entitlement reviews did not identify any issues with terminated users.</i></p> <p><i>ACRO – Two users were previously disabled but were incorrectly re-enabled. These two users did not log on after the termination date. The remaining three users were contractors who had incorrect termination dates entered in the system. Access for all five users has been revoked.</i></p> <p><i>CMS Oracle – The users were contractors. Access has been revoked.</i></p> <p><i>EMS Gateway, CCS, PSOL Siebel, CMS, CDC – The one user was terminated on 5/29/12, but retained access until 6/29/12. Access was removed when detected.</i></p> <p><i>Interconnect – the two terminated users were detected in the Q2 Entitlement Review and their access was revoked.</i></p> <p><i>PSOL Siebel – the majority of these users were contractors. Access has been revoked.</i></p> <p><i>CMS – the two users had very limited access to the CMS application. The access was restricted to setting up projects in a related integrated application. Access has been removed.</i></p> <p><i>CDC – The access of the two users has been revoked.</i></p> <p><i>Active Directory – the user was not removed from an Active Directory due to processing error. This represents 1 user out of 7,000+ active directory users.</i></p>			
<p><i>During the year, Management implemented a new HR information system that will improve the quality of HR data. Management also implemented improvements to the access certification process, including an automated tool for enhanced access governance.</i></p>			
3.03b	<p>A reconciliation between IQNavigator and an HR listing of active employees, contractors, and contingent workers is completed on an annual basis to determine that contractor and contingent worker status is accurate both in IQNavigator and HR. Any discrepancies are researched and corrected in a timely manner.</p>	<p>Inquired of management and was informed that reconciliation between IQNavigator and an HR listing of active employees, contractors, and contingent workers is performed annually.</p> <p>Inspected the supporting documents and determined that the reconciliation between IQNavigator and the HR listing of active employees, contractors, and contingent workers was performed and documented, and that discrepancies were corrected.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
3.04	Logical access for Equifax users to applications, operating systems, and databases is reviewed periodically, in accordance with policy. Access changes are implemented as necessary per the review.	<p>Inquired of management and was informed that access for Equifax users to applications, operating systems, and databases is reviewed quarterly (by Equifax and semi-annually (by IBM), in accordance with policy.</p> <p>For a selection of access reviews for the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, databases, and operating systems, inspected the access reviews and determined that logical access reviews were conducted and that identified access changes were implemented as requested.</p>	Exceptions noted, see below

Exception

- 1 The Q1 and Q2 entitlement reviews were not performed for one of three selected CDC servers. When this server was tested for Q3, it was determined that no users were assigned to that server.
- 2 The Q1 and Q2 entitlement reviews were performed for the EMS Ops, Interconnect and PSOL servers; however 21 of 164 accounts were not reviewed. The Q3 review was performed for all of the 164 users.
- 3 The Q1 and Q2 entitlement reviews were not performed for the selected PSOL database server and the reviewer did not maintain sufficient evidence to demonstrate that the review was properly performed for 2 additional PSOL application servers that were tested. No exceptions were noted for the Q3 review.
- 4 The Q3 entitlement review was not performed timely for the CIS Database.

Management Response: *Within each quarter, entitlement reviews were performed on over 120 servers, with over 45,000 entitlements being reviewed. Reviews are performed at the application, database and server level and over 400 individual system components are reviewed each quarter. The exceptions noted are primarily due to the fact that servers were repurposed within the period due to the nature of the dynamic computing environment and the manual tracking of in-scope servers was not updated on a timely basis.*

During the year, Management implemented a new system to improve the quarterly access certification process. For CDC, EMS Ops, Interconnect

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
<p><i>and PSOL, the Q3 certification was performed using this enhanced process which automatically retains evidence of review and monitors for completion of the access certification. The entitlement review for the CIS database was completed prior to the end of the examination period.</i></p>			
3.05	<p>Privileged access for Equifax and IBM managed applications, operating systems, and databases is limited to authorized individuals.</p>	<p>Inquired of management and was informed that privileged access for Equifax and IBM managed applications, operating systems, and databases is limited to authorized individuals.</p> <p>Inspected system access lists for the applications supporting the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications and determined that privileged access was appropriately assigned based on users' job responsibilities.</p> <p>For a selection of operating systems and databases supporting the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, inspected system access lists and determined that privileged access was appropriately assigned based on users' job responsibilities.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
3.06	<p>Access to implement production application, database, and firewall changes is limited to authorized personnel based on assigned job responsibilities. Access controls systematically enforce segregation of duties between program development and program implementation.</p>	<p>Inquired of management and was informed that access to implement production application, database, and firewall changes is limited to authorized personnel based on assigned job responsibilities with access systematically enforcing segregation of duties between program development and program implementation.</p> <p>For the ACRO and CIS applications, inspected the Endeavor system configurations and determined that access to implement production changes was</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

Equifax's Control Objectives and Related Controls and KPMG LLP's Tests of Controls and Results of Tests

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
		<p>restricted to only those users who require it to perform their job requirements and that users with program development responsibilities were restricted from making production changes.</p> <p>For a selection of servers supporting the CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications, inspected system access reports of individuals with access to implement production changes and determined that access was restricted to only those users who require it to perform their job requirements and that users with program development responsibilities did not have system implement program changes.</p>	No relevant exceptions noted.
<p><u>Results</u></p> <p>Except as noted above, controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 3 are operating with sufficient effectiveness to achieve this control objective.

Control Objective 4

Controls provide reasonable assurance that processing is scheduled appropriately and deviations are identified and resolved in a timely manner.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
4.01	Job scheduling change requests submitted by Equifax are tracked, tested, and authorized by IBM personnel or Equifax management.	Inquired of management and was informed that job scheduling change requests submitted by Equifax are tracked, tested, and authorized by IBM personnel or Equifax management. For a selection of job scheduling changes, inspected supporting documentation and determined that changes were tracked, tested, and appropriately authorized.	No relevant exceptions noted. Exceptions noted, see below.

Exception

The CMS job schedule changes were reviewed and approved by management; however full documentation of the review was not retained.

Management Response: *Additional guidance has been provided to the CMS job scheduling team regarding the documentation of job scheduling changes.*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
4.02	Automated job scheduling tools are used to schedule, process, and monitor production jobs for the applications.	<p>Inquired of management and was informed that automated job scheduling tools are used to schedule, process, and monitor production jobs for the in-scope applications.</p> <p>Inspected the job scheduling tools and logs for the in-scope applications and determined that job failures are monitored and are automatically or manually restarted in the event of a failure.</p> <p>Inquired of management regarding situations where restarting the job does not resolve an issue and was informed that an incident is logged and resolved through the problem management process.</p> <p>Inspected Help Desk procedures and determined that a process for maintaining and monitoring in-scope jobs was documented.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
4.03	A problem management tool is used to track, analyze, and document resolution problems and incidents.	<p>Inquired of management and was informed that a problem management tool is used to track, analyze, and document resolution problems and incidents.</p> <p>For a selection of reported problems, inspected the problem tickets and determined that the following information was included:</p> <ol style="list-style-type: none"> 1) Customer information; 2) Date and time the problem was identified; 3) Date and time the problem was reported, symptom description, and type of problem; 4) Failing resource/component; 5) Actions taken to resolve the problem, including date and time action was taken; and 6) Analysis of initial information to determine appropriate problem record assignment. 	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
4.04	The Root Cause Analysis (RCA) process is used to review significant problems, identify and remedy the source(s) of these problems.	<p>Inquired of management and was informed that The Root Cause Analysis (RCA) process is used to review significant problems, identify, and remedy the source(s) of these problems.</p> <p>For a selection of reported problems, inspected documentation and determined that the RCA process was used to identify and remedy the source problem.</p> <p>For a selection of reported problems, inspected the RCA process and determined that the review included analysis of the root cause, contributing factors, and actions taken to permanently resolve the problem.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
4.05	Problem management meetings are held to review problems, resolutions, and outages on a regular basis. Relevant parties are present at the meetings.	<p>Inquired of management and was informed that problem management meetings are held to review problems, resolutions, and outages on a regular basis. Relevant parties are present at the meetings.</p> <p>For a selection of daily problem management meetings, inspected the meeting minutes and determined that problems, resolutions, and outages were discussed and that relevant personnel were present.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><u>Results</u></p> <p>Except as noted above, controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 4 are operating with sufficient effectiveness to achieve this control objective.

Control Objective 5

Controls provide reasonable assurance that network performance and system capacity are measured and monitored.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
5.01	The IBM Network Monitoring Center is responsible for monitoring network performance for the applications using network-monitoring systems to identify process and batch run performance issues, CPU and memory utilization issues, failed system connections, and backup performance issues.	<p>Inquired with IBM personnel and was informed that monitoring systems were used to monitor and identify issues.</p> <p>Inspected the monitoring system tools and determined that process and batch run performance, CPU and memory utilization issues, failed system connections and backup performance issues were being monitored.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
5.02	IBM prepares a report of network performance trends that is shared at monthly meetings between IBM and Equifax. The report includes root cause analyses for major outages occurring during the month.	<p>Inquired of management and was informed IBM prepares a report of network performance trends that is shared at monthly meetings between IBM and Equifax. The report includes root cause analyses for major outages occurring during the month.</p> <p>For a selection of months, inspected the meeting documentation and determined that system performance, root cause analysis of identified problems, and customer uptime metrics were discussed and reviewed.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
5.03	Internet facing servers are positioned within screened subnets and are protected via stateful packet inspection firewalls.	<p>Inquired of management and was informed that internet facing servers are positioned within screen subnets and are protected via stateful packet inspection firewalls.</p> <p>Inspected the network diagrams and determined that internet-facing servers are positioned within screened subnets and are protected via firewalls.</p> <p>Inspected executive reports from network penetration testing and determined that firewalls include stateful packet inspection.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
5.04	A network scan is performed on a monthly basis.	<p>Inquired of relevant personnel regarding Equifax's security assessment program and was informed that security scans are performed.</p> <p>Inspected the security scanning reports and determined that management reviewed the reports monthly and assessed the results of the scan.</p> <p>Observed that the security report tracked the number of items remediated since the previous month.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><u>Results</u></p> <p>Controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 5 are operating with sufficient effectiveness to achieve this control objective.

Control Objective 6

Controls provide reasonable assurance that programs and data files are backed up.

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
6.01	Backup processes have been implemented and backup procedures are formally documented.	<p>Inquired of management and was informed that backup processes have been implemented and backup procedures are formally documented.</p> <p>Observed IBM personnel perform backup and restoration procedures and noted that backup and restoration processes were implemented and documented to allow backup and recovery of information systems.</p> <p>Inspected backup schedules and determined that technology supporting the ACRO, CIS, CMS, Commercial Credit, CDC, EMS Gateway, EMS Ops, InterConnect, and Personal Solutions applications and databases were listed within the incremental and full backup schedules.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
6.02	Backups for servers are written to virtual tape library.	<p>Inquired of management and was informed that backups for servers are written to virtual tape library.</p> <p>Inspected the replication schedules and rules that are configured in the backup system and determined that the in scope systems are configured to backup through the replication process to an offsite location.</p> <p>Inspected the backup log and determined that backups were successfully performed through the replication process.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

*Equifax's Control Objectives and Related Controls and KPMG LLP's
Tests of Controls and Results of Tests*

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
6.03a	Job scheduling change requests submitted by Equifax are tracked, tested, and authorized by IBM personnel or Equifax management (including backup jobs).	<p>Inquired of management and was informed that job scheduling change requests submitted by Equifax are tracked, tested, and authorized by IBM personnel or Equifax management.</p> <p>For a selection of job scheduling changes, inspected supporting documentation and determined that changes were tracked, tested, and appropriately authorized.</p>	<p>No relevant exceptions noted.</p> <p>Exceptions noted, see below</p>
<p>Exception</p> <p>The CMS job schedule changes were reviewed and approved by management; however full documentation of the review was not retained.</p> <p>Management Response: <i>Additional guidance has been provided to the CMS job scheduling team regarding the documentation of job scheduling changes.</i></p>			
6.03b	Periodically test restorations of data are conducted for a sample of critical data to verify the integrity of the data backup processes.	<p>Inquired of management and was informed that test restores are conducted periodically for a sample of critical data to verify the integrity of the data backup processes.</p> <p>Inspected a completed restoration request and determined that the restoration was performed successfully.</p>	

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
6.04	Automated job scheduling tools are used to schedule, process, and monitor production jobs (including backup jobs).	<p>Inquired of management and was informed that automated job scheduling tools are used to schedule, process, and monitor production jobs for the in-scope applications.</p> <p>Inspected the job scheduling tools and logs for the in-scope applications and determined that job failures are monitored and are automatically or manually restarted in the event of a failure.</p> <p>Inquired of management regarding situations where restarting the job does not resolve an issue and was informed that an incident is logged and resolved through the problem management process.</p> <p>Inspected the Help Desk procedures and determined that a process for maintaining and monitoring jobs was documented.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

#	Controls Specified by Equifax	Testing Performed by KPMG	Results of Control Tests
6.05	A problem management tool is used to track, analyze, and document resolution of problems and incidents (including backup jobs).	<p>Inquired of management and was informed that a problem management tool is used to track, analyze, and document resolution problems and incidents.</p> <p>For a selection of reported problems, inspected the problem tickets and determined that the following information was included:</p> <ol style="list-style-type: none"> 1) Customer information; 2) Date and time the problem was identified; 3) Date and time the problem was reported, symptom description, and type of problem; 4) Failing resource/component; 5) Actions taken to resolve the problem, including date and time action was taken; and 6) Analysis of initial information to determine appropriate problem record assignment. 	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><u>Results</u></p> <p>Controls operating as described.</p>			

Based on the tests of operating effectiveness described above, the controls tested for Control Objective 6 are operating with sufficient effectiveness to achieve this control objective.

Section V

Other Information Provided by Equifax Inc.

Revenue, Business Continuity and Disaster Recovery Program, Insurance Coverage

The information in this section describing Equifax's revenue volume, business continuity and disaster recovery program, and insurance policy coverage is presented by Equifax to provide additional information and is not a part of Equifax's description of controls that may be relevant to user entities' internal control. Such information has not been subjected to the procedures applied in the examination of the description of controls applicable to the processing of transactions for user organizations and accordingly, KPMG expresses no opinion on it.

REVENUE

The following information is intended to provide user organizations with an understanding of the relative revenue volume associated with the key applications addressed within this report.

Applications	% of Annual Revenue Volume
ACRO	49%
PSOL	24%
CMS	17%
EMS Gateway and EMS Ops	8%
CDC	1%
Commercial Credit	1%

CIS is the core billing and invoicing system for these applications and is not listed above.

BUSINESS CONTINUITY AND DISASTER RECOVERY PROGRAM

OVERVIEW

Program Overview

Equifax is acutely aware of the importance of the services and data we provide to our customers and recognizes its responsibility to maintain programs designed to increase the assurance of their continued availability. In order to mitigate the risk of unplanned disruptions in service to our customers, Equifax has a business continuity program composed of a subordinate Business Resumption Program, Disaster Recovery Program, and Crisis Management Program.

With respect to information technology, Equifax has sought to mitigate the risk of outages through the robust engineering of its systems and the infrastructure which supports its data centers.

Should, however, a disaster¹ occur, a Disaster Recovery Program is in place and designed to restore our critical information technology systems and services. The program is designed to efficiently handle numerous types of disasters, to include complete loss of a data center.



Risk Mitigation Approach

Equifax's Alpharetta, Georgia data center is a modern data center with:

- state of the art electrical and mechanical systems with auto monitoring;
- fire detection and suppression systems supplemented with dry pipe fire suppression and dry-chemical fire extinguishers;
- 7x24 staffing; and,
- high availability system architectures to mitigate the risk of outages.

Disaster Recovery

Critical applications and key information technology infrastructure nodes are assigned one of the Equifax standard Disaster Recovery Tiers. Disaster Recovery Tiers have provisioning requirements, Recovery Time Objective (RTO), and Recovery Point Objectives (RPO).

Disaster recovery planning and preparations include:

- A clear definition of, and strategy for, meeting RTOs and RPOs (where applicable) for each application provisioned for disaster recovery.
- Use of geographically diverse recovery sites with all locations maintaining comparable levels of physical and access security controls.
- Documentation and provisioning designed to increase the assurance that recovery of critical systems in a worst-case scenario involving loss of the primary facility, with plans written in sufficient detail that they may be implemented by personnel not familiar with the system.

¹ A disaster is any event beyond Equifax's reasonable control which precludes Equifax from performing its critical business functions/services.

- Procedures for disaster recovery declaration, plan implementation, activation of the recovery site(s), and notification of employees, vendors, clients and service providers of the invocation of the Plans.
- An annual schedule for testing and maintaining Disaster Recovery Plans, and procedures for incorporating results from tests into the next scheduled revision of the Plans.²

Equifax currently has a team of trained, experienced, employees whose role is to manage and oversee the Disaster Recovery Program.

Customer Reviews and Discussions

Equifax customers may send a request to the Disaster Recovery group (Global_DR@equifax.com) and request:

- to review the data center disaster recovery plan³ on site;
- a summary of an application's most recent test results, or;
- a web presentation or discussion on the disaster recovery planning, provisioning, and/or testing with the Disaster Recovery Staff.

Business Continuity and Resumption

In the event of a catastrophic disaster, Equifax has identified key business objectives that require immediate recovery support and resources. These key business objectives are:

- Restore operations of critical business processes and systems according to their assigned criticality tier with corresponding RTOs and RPOs.
- Maintain confidence of employees, customers, and stakeholders
- Maintain service levels for customers
- Provide support for daily operations through alternative workarounds
- Mobilize the Crisis Management Organization in order to increase the assurance that continuity of business operations when appropriate

Equifax is responsible for the overall Global Business Continuity Program. Guidelines, policies, and other tools are used for the planning, development, implementation, testing, and maintenance of the plans. These plans address emergencies ranging from natural disasters, pandemics, and man-made disasters. Testing of the plans is done, at a minimum, on an annual basis utilizing various exercises from actual full evacuations to tabletop drills. Plans are reviewed and updated on an annual basis as well as after tests, when business functions change, and/or employment changes or physical facility changes have taken place. Crisis Management is incorporated into our Business Continuity Program and follows the same approach.

² Equifax reserves the right to change any of its Plans or related policies at any time.

³ Plan reviews are subject to Equifax's security and confidentiality requirements and must occur within the data center; no copies of the disaster recovery plan will be permitted to be taken off site.

INSURANCE POLICY COVERAGE

Equifax maintains a comprehensive property and casualty insurance program suitable for the risks associated with its business. The program is designed to minimize the adverse financial impact associated with losses related to the Company's services, operations, personnel, buildings, equipment and potential legal liability. Insurance policies purchased include, property insurance, business interruption, professional liability, technology and internet privacy, general liability, auto liability, excess liability, crime, worker's compensation, and employer's liability. Equifax employs a Director of Risk Management responsible for the design and implementation of the insurance program. Equifax and its insurance broker conduct annual reviews prior to the renewal of each policy to ensure the policies are adequate based on the Company's risk profile. Insurance renewal recommendations are discussed with the Senior Vice President and Treasurer. Major program recommendations, as well as the overall program design, are reviewed by the Chief Financial Officer. Equifax maintains insurance coverage mandated by State and Provincial law for worker's compensation and auto liability.