Talent Logic, Inc. **("VENDOR")**

STANDARD OPERATING PROCEDURES FOR CONTINGENT WORKERS: PRIVACY AND PROTECTION OF PERSONAL DATA AND BUSINESS CONFIDENTIAL INFORMATION

NOTE: THIS DOCUMENT IS APPLICABLE TO VENDOR COMPANIES AND CONTINGENT WORKERS

VENDOR -- PLEASE REVIEW AND ENSURE YOU SATISFY THESE STANDARD OPERATING PROCEDURES.

Standard Operating Procedures for Contingent Workers: Privacy and Protection of Personal Data and Business Confidential Information v2.0	
Supersedes: Standard Operating Procedures for Vendor and any of Vendor's Employees Providing Services to a First Data Entity: Privacy and Protection of Personal and Business Confidential Information v1.0	
Policy Owner: Deanne Klepper	**Policy Custodian:** David Tomlinson
Distribution: All Contingent Workers	**Issued By:** John Atkins
Approved by: John Atkins, Susan Mauldin	**Approved Date:** March 1, 2013
	Effective Date: March 1, 2013
	Next Review Date: March 1, 2014

TABLE OF CONTENTS

STANDARD OPERATING PROCEDURES FOR CONTINGENT WORKERS: PRIVACY AND PROTECTION OF PERSONAL DATA AND BUSINESS CONFIDENTIAL INFORMATION

Purpose

These Standard Operating Procedures ("SOPs") describe the limits on the use and disclosure of personal data and business confidential information belonging to First Data Corporation, its affiliates, or subsidiaries, ("First Data") as defined herein. These SOPs apply to Personal Data and Business Confidential Information whether in paper, electronic or other form. This document is intended to supplement any written agreements between First Data and the Contingent Worker or Vendor.

Definitions

Personal Data is defined as a consumer's, employee's or client's individual name (this does not include a business' name unless local laws require otherwise), address, date of birth, telephone/fax number, e-mail address, URL, IP address, Social Security Number, Personal Identification Number, account number, certificate/license number, vehicle identifiers, biometrics identifiers or other genetic information, photographic images, transaction information, CVV/CVC, personal data revealing racial or ethnic origin, political opinions and membership in political associations, religious beliefs and affiliations, philosophical beliefs, trade-union membership, criminal records, sexual preferences, data concerning health, including but not limited to, any information about health status, provision of health care, or payment for health care that can be linked to an individual, any other personally identifying characteristics or codes, or any other data or combination of aforementioned data relating to a consumer, employee, client (excluding business name unless local laws requires otherwise) or a transaction collected and stored by First Data Corporation ("First Data") as a result of First Data's performance of services for its clients or otherwise in the course of conducting its business.

Business Confidential Information ("BCI") is information that does not include or constitute Personal Data but is information that if disclosed outside of First Data, would adversely impact First Data, its business partners and/or its clients. Examples include financial data, acquisition or divestiture plans, strategic sales or product plans and information regarding pricing and development roadmaps, Employer Identification Number, contract information, programming techniques and any other proprietary information. BCI includes information classified as Internal Only, Confidential, or Restricted, as defined by First Data's Information Security Policy. For more information, consult First Data's Information Security Policy listed on FirstWeb or available from the First Data Business Contact.

First Data Information is both Personal Data and BCI.

Privacy Officer is a First Data Privacy Officer, Champion and/or employee appointed by the management team of his or her business unit or shared services group to assist the First Data's Privacy Office and executive management in administering First Data's privacy programmes, including utilization of the Monthly Mini Audits.

Vendor means Talent Logic, Inc. .

Contingent Workers collectively refers to all workers who provide services to First Data and who are NOT paid via a First Data payroll, including Independent Contractors and Leased Workers. Contingent workers can include both workers through a Vendor's payroll or Independent Contractors.

Business Contact is the First Data employee or employees who engage the Contingent Worker and oversee the Contingent Worker's provision of services to First Data.

Scope

This document applies to all Contingent Workers, wherever their location, supporting First Data Corporation and its subsidiaries.

Limitations on Data Usage

First Data limits access to Personal Data and BCI stored by it to those persons who need access to that Personal Data and/or BCI to fulfill their responsibilities. Hence, Personal Data and/or BCI of First Data should be used for the following purposes:

- Perform services for First Data business units or other shared services units in their capacity as a Contingent Worker.
- Resolve issues and incidents involving the provision of services to First Data or at First Data's request.
- Implement projects or conduct other activities under the contract governing provision of services.
- Document system functionality.
- Consult with and/or train First Data's employees and/or clients.
- As otherwise permitted by First Data policy.

Contingent Workers with access to Personal Data and/or BCI at First Data are forbidden from accessing or using that Personal Data and/or BCI for personal reasons or for any purposes other than fulfilling their responsibilities under the contract governing provision of services to First Data. In addition, prior to utilizing First Data's or its clients' Personal Data and/or BCI, all Contingent Workers must ensure that such usage is permitted under applicable contracts. These requirements help protect First Data, its employees, clients and business partners since First Data processes Personal Data of those various parties from time to time. Furthermore, these requirements facilitate First Data's compliance with its written agreements or with instructions from its clients or business partners (as applicable), in compliance with applicable laws and in compliance with First Data's applicable policies as amended from time to time.

In order to fulfill those various obligations, Personal Data and/or BCI must be accessed and used only as necessary, or in compliance with applicable laws, contracts and policies. If a Contingent Worker is not sure whether particular access or use of Personal Data or BCI is necessary, that Contingent Worker should consult with First Data's Privacy Office, legal department, or his or her Business Contact for clarification.

The requirements of this SOP relating to First Data Information are in addition to, and not in place of, any other Vendor Minimum Requirements established via contract or First Data policy.

Owner

This document is owned by First Data Corporation. Development of this document was a collaborative effort and is the joint responsibility of First Data's Privacy Office, the Enterprise Security, Risk and Compliance ("ESRC") group, and First Data's business unit and shared services Privacy Officers.

Vendor Management Team Responsibilities

The management teams within the Vendor's organization shall be responsible for:

- Ensuring that all Contingent Workers comply with this SOP.
- Addressing, in conjunction with appropriate stakeholders from First Data, each violation of these SOPs with the appropriate care which may include an investigation of the violation, prompt remedial action, and steps designed to prevent future occurrences of the violation.

- Ensuring that any Contingent Worker has successfully passed a background check in compliance with First Data's requirements.
- Providing information to First Data regarding changes to a Contingent Worker's job function, access permissions or scope of duties and submitting changes in a timely manner to the appropriate First Data stakeholders:
    - upon a change in the Contingent Worker's job function;
    - upon a departure, transfer or addition of a Contingent Worker; or
    - upon a significant change to the underlying business or clients served by a Contingent Worker.
- Ensuring that First Data's termination processes are followed for departing Contingent Workers including, but not limited to,:
    - properly returning all First Data issued equipment (laptop, Personal Digital Assistant device, Smartphone, etc.), keys, badges, tokens, etc.;
    - immediately notifying the proper teams regarding disabling the Contingent Worker's Access Profile and/or SSL VPN access; and
    - immediately notifying the proper teams regarding disabling the Contingent Worker's ability to access non-public areas of First Data buildings.
- Abiding by the terms of the agreement between Vendor or Contingent Worker and First Data.
- Providing First Data with a copy of the Statement of Understanding for all Contingent Workers assigned by Vendor to First Data upon First Data's request.

If the Contingent Worker is an independent contractor providing services directly to First Data, it is the responsibility of the Contingent Worker's Business Contact at First Data to fulfill all duties and responsibilities outlined above including, but not limited to, obtaining a signed copy of the Statement of Understanding for Contingent Workers and making that form available to First Data management upon request.

Responsibilities of Contingent Workers Assigned to First Data

It is the responsibility of each Contingent Worker to follow these procedures and take appropriate actions to protect First Data's Personal Data and/or BCI.

All Personal Data and/or BCI shall be treated as confidential, subject to disclosure to and discussion with only those First Data employees or Contingent Workers who have a need to know such information.

A Contingent Worker becoming aware of a proposal to transfer Personal Data or BCI to third-parties and/or across country borders should inquire as to whether the First Data Privacy Office or his or her local Privacy Officer has approved the proposed transfer. Information about First Data's Data Across Borders Program is available on FirstWeb or via your First Data Business Contact.

The following lists of requirements are not all-inclusive. Therefore in addition to complying with all applicable policies and the requirements contained in these SOPs, Contingent Workers are expected to use their best judgment and to consult their First Data Business Contact when determining how to protect Personal Data and/or BCI, and when applying the need to know and minimum necessary standards before disclosing Personal Data and/or BCI.

Information Access:

- Access Information: Access to Personal Data and/or BCI must be restricted to the minimum necessary to perform expected job functions. Changes to access will be requested and approved by appropriate designee. Where possible access rights should be based on the role performed, not on the individual performing the role to avoid unintentional access issues.
- Consumer Calls: If a consumer contacts any Contingent Worker, the Contingent Worker will refer the call to a First Data employee who will ask appropriate questions to find out where to direct the caller. Under no circumstances should Personal Data be given directly to a consumer except by those authorized to do so upon proper verification or authentication of caller. Where Contingent Workers are providing Call Center services, the Contingent Worker will follow instructions as given by Call Center personnel relating to consumer calls.
- Need to Know Basis: Documents containing Personal Data and/or BCI should only be shared with individuals on a need to know basis. Confidential information should not be discussed outside of the work environment. Collection, printing, disclosure of, use of, and access to Personal Data and/or BCI must be limited to the minimum necessary to perform required functions and only within approved processes.
- Unauthorized Removal: If a Contingent Worker suspects an individual is trying to remove equipment, Personal Data or BCI from a work area or building without appropriate management approval, the Contingent Worker should immediately report the issue via telephone to the **FDC Corporate Security and Data Privacy Hotline**. The Hotline is available 24 hours a day at the following numbers: **(888) 427-4468** and **+1 (402) 777-2911**.
- User ID Passwords: All user IDs and passwords or any type of access device should not be accessible to, or used by, anyone except the authorized user (i.e. avoid distribution of user name, system, and password in a single email or same file – utilize multiple communication methods to disseminate information to end user or user's manager). For example, do not have passwords displayed on or near computers or other security devices. NEVER share the user ID or password with anyone with the exception of required maintenance by an FDC LAN administrator.
- Verification of New Contacts: Verification of new contacts at client locations should follow the established new contact procedure for each First Data business unit.

Storage / Retention / Destruction:

- Disks or CDs: Personal Data and/or BCI sent outside First Data on a storage device such as a computer disk or CD must be encrypted. Electronic media should be properly labeled with a destruction date according to the Information Classification stated in the First Data Information Security Policy (available on FirstWeb or through the First Data Business Contact).This information should be sent in a manner whereby each physical transfer of media is logged and signed by the intended recipient unless the recipient or data owner provides other instructions in writing regarding delivery and such arrangement is approved by First Data management.
- Return of Information: Upon removal from or completion of the assessment, the Vendor or Contingent Worker should return all Personal Data or BCI collected while providing services to First Data.
- Disposal: All printed materials containing Personal Data and/or BCI must be disposed of in accordance with First Data's Records Retention Schedule and Security Standards listed on FirstWeb or available through the First Data Business Contact. If a First Data provided disk shredder or secure disposal service is not available, CD/DVD/floppy disks must be scratched through, cut up or bent in half with the discarded pieces placed in more than one trash bin.
- File Cabinets: All file cabinets and team lateral file cabinets must be secured after business

hours and during prolonged absences from an office or work station during business hours.

- Keys: All files containing Personal Data (including but not limited to personnel files) must be stored in a locked file cabinet or office and the key stored in a secure location. Authorized personnel must keep master keys in a secure location. Keys must not be left in the open or anywhere the keys may be easily found.
- Record Retention: Any record of Personal Data and/or BCI should be held for the minimum amount of time necessary and in accordance with First Data's retention requirements under First Data's Records Retention Schedule and Security Standards for that particular record unless subject to a litigation hold.
- Recycle and Shredder Bins: Security waste bins should be locked and the contents confidentially destroyed by shredding. All materials containing Personal Data and/or BCI should be only disposed of in locked security waste bins. Personal Data and/or BCI should not be disposed in non-security waste and/or open recycle bins. Personal recycle bins should be emptied nightly and the contents distributed to either a recycle bin or security waste bin, depending on the contents of the document.
- Storage of Personal Data and/or BCI: Personal Data and/or BCI needs to be adequately protected wherever it is stored. Laptop computers and other portable electronic devices containing Personal Data and/or BCI must be encrypted. All persons storing Personal Data and/or BCI on network or shared drives must confirm that only individuals with a business need have access to that Personal Data and/or BCI.

Meetings:

- Grease/White Boards: Grease or white boards with Personal Data and/or BCI written on them should be erased immediately when they are no longer required for work functions and in all cases prior to the end of any meeting. They should never be viewable from an exterior window.
- Meetings: Meetings held with clients discussing Personal Data and/or BCI should only include those individuals necessary for the discussion. Discussions involving specific Personal Data and/or BCI should not occur in a common area or anywhere outside the secure workplace setting.
- Meeting Materials: Whenever Personal Data and/or BCI are used for meetings, it is the responsibility of the meeting leader to verify no materials containing such information are left in a conference room. The excess material should be disposed of in locked shredder bins.
- Presentations: Materials (including, but not limited to, slides, training, packets, screen shots) containing Personal Data will be scrubbed to verify Personal Data is removed or modified so it cannot be linked to the person it references unless that person consents to such use in writing in a form approved by the local legal department. BCI shared in presentations should not contain more confidential information than reasonably necessary and should not be distributed more widely than reasonably necessary. Cover pages of presentations or notification to recipients should include reference to the Personal Data and/or BCI contained within and a requirement to maintain the confidentiality of that information.
- Speakerphones: Meetings held over speakerphones will be in a room with the door closed. Contingent Workers should utilize appropriate volume levels to minimize the possibility of confidential conversations being overheard.

PC / Software / Office Equipment:

- Collaboration Tools: Access to folders/files house on common (shared) drives or SharePoint will be limited to the minimum necessary to perform assigned job functions. Common Drive owners and SharePoint site owners should perform an annual audit to verify access is

granted only to those who have a need to know and that proper retention schedules are being adhered to.

- Emails: Any internal emails or other electronic communication, including but not limited to text messages, containing Personal Data and or BCI should not be transmitted unless it is necessary for a specific business purpose. If transmission is required, Personal Data and/or BCI must be deleted before sending, using the "minimum necessary" and "need to know" standards. When there is a legitimate business reason to email Personal Data to an external party it must be encrypted using one of the approved email encryption methods described in Appendix A. Emailing, texting or otherwise transferring First Data Information from a company messaging account to any non-First Data email account (including Vendor company email or personal email) is prohibited.

  Any Personal Data that is emailed to an external party must be encrypted or sent via secure email as detailed in Appendix A. Please refer to the First Data End User Policy (available on FirstWeb, through a member of the First Data Business Contact) for additional information as to how to send an encrypted email.

- Fax Machines/Copiers/Mail: All documents containing Personal Data and/or BCI should be removed and/or filed immediately from fax machines, printers, scanners, copiers and mailboxes in the workplace. It is the responsibility of each individual to remove his or her documents during business hours. At the end of the day, documents left on printers and fax machines must be disposed of in locked recycle bins by the department administrative assistants or other designee. Materials transmitted/received after end of shift/end of business hours should be picked up by teams immediately in the morning of the next workday. The administrative assistant or designee will check at the end of the day to verify that materials with Personal Data and/or BCI are not left in mailboxes unless enclosed in an envelope. All fax transmittals should contain a cover with the sender contact information and a disclaimer that if receiver is not the intended recipient the fax should be destroyed immediately and to contact the number on the cover sheet to inform of the error. As a best practice, full account numbers or other Personal Data should not be faxed. Consult the local First Data Privacy Officer if you are sending a fax internationally or if you have a situation where you believe the faxing of this type of data is necessary to establish a procedure with adequate safeguards for transmitting the data.

- Laptop Policy: Contingent Workers are required to secure any unattended portable electronic device (e.g. laptop, PDA device, Smartphone, First Data issued tablet, etc.) that contains First Data's Personal Data or BCI by locking the device in an office or inside a desk. All laptops or other portable devices are required to have a First Data authorized encryption program installed and operational. If the device is taken outside the general work area, it must be kept secure at all times. Remote Contingent Workers should keep laptops in a secure area after hours. First Data issued laptops must not be used by anyone except the assigned Contingent Worker (for example, other members of the individual's family must not utilize First Data equipment).

  Vendor Contingent Workers may only use a Vendor issued portable electronic device or other non-First Data equipment with the express written permission of First Data's ESRC. If a Vendor Contingent Worker is utilizing an ESRC approved Vendor issued portable electronic device, the Contingent Worker must follow all applicable policies and procedures for securing the equipment and the data housed therein and must in all cases utilize commercially reasonable means of protecting all First Data Information housed thereupon.

- Software: Only First Data provided or approved software should be housed/downloaded on desktops or laptops issued by First Data to Contingent Workers. Contingent Workers should not download software for screensavers, wallpaper, shareware, or freeware onto First Data issued desktops or laptops without proper authorization to reduce the risk of virus infections, malware attacks and violations of intellectual property law.

Workspace / Physical Environment:

- Delivery of Documents: When placing a document with Personal Data and/or BCI on a desk, inbox or other visible area the document should be covered, turned over, placed into an interoffice envelope, or otherwise reasonably protected from view. Documents containing Personal Data and/or BCI should never be left by a window or in plain view. Any interoffice envelope containing Personal Data and/or BCI should be taped such that the end recipient can easily determine if the contents may have been otherwise compromised. If the recipient believes that the contents have been compromised, the recipient should contact the sender to determine the exact contents and then contact the **First Data Security and Data Privacy Hotline** for assistance. Any confidential or sensitive media being distributed to an external entity should be sent secured carrier such that the receiving entity must sign for the delivery unless the recipient or data owner provides other instructions regarding delivery.
- Home or Other Offsite Access: All offsite access to any First Data network must go through First Data's SSL VPN connection using a SecurID token or other connection (such as VDI) as approved by First Data. All Contingent Workers must limit retention of Personal Data and/or BCI to the minimum amount and time necessary and, unless subject to a litigation hold, such Personal Data and/or BCI must be deleted when no longer needed for First Data functions. Transferring Personal Data and/or BCI to a non-First Data email account or to any device not pre-approved by First Data is prohibited. Reasonable steps must be taken at all times to ensure that Personal Data and/or BCI (whether paper or electronic) is not viewed by any person who is not authorized to view such Personal Data and/or BCI.
- Lock Workstations: Contingent Workers are to lock workstations (Ctl/Alt/Del) when leaving the workstation at any time.
- Web Sites: Personal Data and/or BCI should not be accessible on any First Data web site unless access is restricted with a password or other compensating controls deemed sufficient by the First Data ESRC group.
- Workstation/Office Area: All materials or media (including but not limited to paper, CD-ROM, floppy disks, USB drives, etc.) containing Personal Data and/or BCI are to be secured in a locked cabinet or room when unable to monitor. Personal Data and/or BCI should be removed from clear view at the end of the work day. If an office contains Personal Data that is not secured in a locked desk/cabinet, the office door must be locked (during non-business hours) and the trash can placed outside the office door for emptying. Keys to workstations, offices and file cabinets are not to be visible or left in the locks.

Other:

- Call Recording: Any recording of conversation must be announced unless an exception has been approved by a Senior Vice President of the applicable First Data business unit or shared service group after consultation with the legal department. Recordings containing Personal Data and/or BCI should not be distributed via wave (.wav) or audio video interleaved (.avi) type files. Persons who need to transmit such files should contact the local First Data Privacy Officer to discuss appropriate ways to do so.
- Cameras: Cameras are permitted in the workplace if they are associated with CCTV monitoring of secure areas or if they are required for a Contingent Worker to accomplish their job activities and with supervisor approval. Cameras, or any other device incorporating an ability to store images, may not be used to transmit content or images containing Personal Data or BCI.
- Outside of Work: Contingent Workers should take reasonable steps to safeguard Personal Data and/or BCI when verbal discussions take place outside of the department's business area. When transporting materials containing Personal Data and/or BCI outside of the work environment, documents cannot be visible to others (i.e. in an envelope, folder, Blackberry or

briefcase). Persons who leave these materials in a vehicle untended must use reasonable efforts to guarantee the security of the materials (lock vehicle door, etc.). If Personal Data and/or BCI is misplaced, lost, stolen or otherwise becomes unaccounted for, or is in any way known or suspected to be accessed by an unauthorized party, the Contingent Worker must immediately report the issue via telephone to the **FDC Corporate Security and Data Privacy Hotline**. The Hotline is available 24 hours a day at the following numbers: **(888) 427-4468** and **+1 (402) 777-2911**.

Security Breach/ Privacy Incident Notification

Security Breach: Any known or suspected Information Security incident, as defined by First Data policy, must be reported immediately via telephone to the **First Data Security and Data Privacy Hotline**. The Hotline is available 24 hours a day every day at the following numbers: **(888) 427-4468** and **+1 (402) 777-2911**. When calling the hotline, be prepared to provide the following information; your name, what happened, your work location, where you are located (not where your office is located, but where you are physically located), and where you can be reached (mobile number if available as well). The operator will immediately contact the on-call Corporate Security representative. Calls received on the Hotline will be directed to the proper parties for response.

STATEMENT OF UNDERSTANDING

I, _____ , an employee of Talent Logic, Inc. understand that:

I am responsible for reading, understanding and complying with these Standard Operating Procedures for Contingent Workers including any and all attachments, exhibits, appendices, etc.

I am responsible for contacting my First Data contact for any clarification of any of the policies in this document;

I am responsible for notifying my First Data Business Contact and/or such other responsible parties if I become aware of or have reason to believe that a violation of these Standard Operating Procedures for Contingent Workers has occurred, or may have occurred, or Personal Data and/or Business Confidential Information has been accessed, or may have been accessed, by an unauthorized person;

I understand that these procedures may be revised at any time and that my employer may require an updated Statement of Understanding from me at such time; and

If I do not follow the procedures set forth in these policies during my assignment on the First Data account, I may be subject to corrective action from my employer, which may include, but not be limited to, removal from the First Data account.

Please complete the following information to certify your Statement of Understanding:

_____
Contingent Worker Name

_____
Contingent Worker ID Number
(Vendor Issued Number - N/A for Independent Contractors)

_____
Contingent Worker Signature

_____
Date

APPENDIX A:
EMAIL SECURITY - HOW TO SEND ENCRYPTED EMAIL

Note – please consult your local Information Security or Privacy Officer staff regarding local procedures as the process may vary by location.

For further information, please consult the End User Policy.

Internet Mail Encryption

As you know, Personal Data, BCI and/or PCI data sent over the internet must be protected from unauthorized access or tampering. First Data offers differing methods of securing email depending on where you are located:

- server-to-server session encryption
- domain-to-user *FDCSecureMail:*
- securing production mail

We also offer the automatic encryption of reports generated and emailed out from production applications. Each of these methods and how to use them are described below.

Server-to-Server Session Encryption

(Available in the United States, United Kingdom, Ireland, Germany and Austria)

(Not available in all other countries)

First Data can automatically secure email to any email server that can support TLS/SSL session encryption. A growing number of customers and business partners are asking that First Data ONLY sends emails securely. This is called Enforced TLS. When First Data enforces TLS with another organization, email will be held in queue if for any reason a secure session cannot be established. Once the problem is resolved, the message is sent.

For everyone using a firstdata.com email address - Companies that have an Enforced TLS agreement with First Data, along with a list of domains with whom we securely route through private channels, is listed on FirstWeb here. Different regions may have additional links so contact your local Information Security Officer if you have additional questions.

All employees not using a firstdata.com email address should contact their local Information Security Officer to receive information specifying with which customers or business partners they can exchange secure emails using Server-to-Server session encryption.

If you routinely email a particular company and would like to discuss secure mail routing with them, you can request Enforced TLS through the IT Service Request Catalogue.

Domain-to-User *FDCSecureMail:*

(Available in the United States, United Kingdom, Canada, Argentina, Brazil, Uruguay, Colombia, Panama, Mexico and Ireland)

(Not available in all other countries)

If you are emailing Personal Data, BCI and/or PCI data to a company not utilizing Enforced TLS, PGP or SMIME encryption, you must protect that message with *FDCSecureMail:*. To do so, include *FDCSecureMail:* in the Subject line of your message, followed by whatever other text you choose.

Everything that goes out the external gateway with *FDCSecureMail:* in the subject line will be secured. Other than internet web access, the recipient does not need any special software or computer setting to receive or read the message.

FDCSecureMail: from the Recipient's Perspective

The first time a customer receives an *FDCSecureMail:* message, he/she will be asked for “Password” and “Confirm Password.” The recipient will then be presented with three challenge response questions that

will be used if password recovery is later required. Upon the next login, only the “Password” field will be displayed.

Support for those who send or receive an *FDCSecureMail:* message is provided by the Response Center at 1-800-337-1222. Select Option "3" to talk to a Response Center Representative and then option “2” for customer service.

If you are emailing Personal Data BCI and/or PCI data to a company not able to utilize any of the above mentioned methods, you need to contact your security representative to discuss an approved exception.

Everything that goes out to external parties that is of sensitive nature must be secured.

Securing Production Mail

(Available in the United States and United Kingdom)

(Not available in all other countries)

Production systems that generate external email containing Personal Data must be coded to include *FDCSecureMail:* in the subject line OR the message can be secured whenever an agreed upon file name is found in an attachment. Please note that ALL production systems that generate email must be registered with the corporate Messaging Group. If you wish to register a system, please obtain a request form by contacting the PCLAN Support Helpdesk at 1-877-332-4526 (U.S.) or +44 (0) 1268 296989 (U.K.) and open a First Data Messaging ticket.