



Local Government Corporation *Information Security*

March 24, 2009

LGC Valued Customer,

With the ever-changing environment today, it is vitally important to protect your customer's private information. On May 1st of this year, the *Fair and Accurate Credit Transactions Act* (FACTA) goes into effect. FACTA, as it is commonly known, requires anyone who extends credit to put policies in place to protect their customer's private information. The Act considers anyone who offers deferred payments for goods or services such as utility payments, as a creditor. The primary purpose of this Act is to identify any attempted theft of a customer's identity. This information includes date of birth, address, and Social Security Number, just to name a few. In addition, FACTA identifies *26 Red Flag Rules* provided as guidelines for things to consider when developing this policy. Much information is available via the Internet or various support agencies, such as MTAS or CTAS. Please consult one of these sources for any specifics regarding your entities requirements.

Furthermore, we believe it is extremely important to protect your employees' private information. While this is not required in FACTA, we believe it makes good sense. In addition to the information stored on paper in your office, your LGC software also contains information that could be considered sensitive. You should take every precaution to ensure any information considered sensitive is protected from any potential misuse, such as identity theft. The information required by FACTA is a good starting point for protecting sensitive information.

LGC has identified several computer-generated processes that contain employee's sensitive information. These processes are identified as an overall part of our policy, and are listed on our website. We recommend you contact each institution with which you exchange such information to determine if you are already using a secure method of transfer, or if there is a recommended secure transfer method of which you may not be aware.

From time to time, it may be necessary for our staff to obtain a copy of your data in order to accurately identify and correct a software issue. This information will not be taken without your prior knowledge and consent. We take our responsibility as your software vendor very seriously. Our employees treat all of our customer's information with respect and do our very best to protect your employees' privacy. A copy of our policy regarding the protection of your data is available via our website, www.localgovcorp.com.

Also, if there are any questions regarding information generated on your computer by LGC software, please do not hesitate to contact us.

Respectfully,

Local Government Corporation



Local Government Corporations Internal FACTA Policy

The below policy was established to ensure compliance with The Fair and Accurate Credit Transaction Act of 2003 (FACTA). For additional information and assistance, visit <http://www.privacyrights.org/fs/fs6a-facta.htm#1>

The two primary areas of concern are remote connectivity and data security.

LGC policy on remote connectivity

Sometimes it may be necessary for LGC to connect to customer computer systems remotely to help with issues related to software, hardware, or network connectivity. LGC requires a secure connection to its customers and each employee is required to follow specific guidelines.

There are three methods we could use for this connectivity which are outlined below.

A. Modem Access: Some LGC customers utilize modem support through a telephone line because of cost or they are unable to get high speed internet access in their area. In these situations, customers follow these procedures:

1. The modem is to be turned off when not being used.
2. The customer must request LGC to connect to their system and a login and password is used to protect the customer.
3. Once LGC is finished, the customer turns off their modem.

B. Bomgar: To protect the integrity of the customer's screen data and prevent unauthorized eavesdropping and/or modification of application data in transit, Bomgar uses 256 bit SSL to encrypt all application communications in transit. In addition, in order for LGC to have access to your system, the session must be initiated by the customer to ensure access is acceptable and authorized for support. There is not a way for LGC to start a Bomgar connection from LGC to a customer machine. This must be done by the customer, giving LGC access to their system.

C. Customers on LGC Network Support: LGC offers a paid support feature where LGC oversees, monitors, and supports your entire network infrastructure. Although software support is generally handled under the Bomgar option above, network support customers are connected to our network via IPSEC Virtual Private Network (VPN). The VPN tunnels under this option allow us to oversee the functionality and health of your network. The encryption is multi-layered, with the initial phase using 3DES encryption. The second phase connects with DH Group2 (1024bit) encryption. These connection phases are renegotiated at intervals that ensure the keys are kept secure and change on a regular basis.



LGC's Handling of Customer Data

All customer data is handled in accordance to LGC's Corporate Policy Manual.

Backup copies of customer databases are sometimes stored on LGC computer systems for use in resolving support issues, testing for software bugs, and aiding in developing new software features. Many of these databases contain confidential data such as social security numbers, driver's license numbers, bank account numbers, etc. Confidential data is also obtained when computer systems are exchanged or disk drives replaced. This policy defines the procedures Local Government Corporation personnel will follow to insure that all confidential data acquired from an outside source is secured and/or destroyed for protection from identity theft.

When a customer's database is transferred to an LGC computer, data scrambling software will be run to scramble all the confidential data. The data scrambling software will change the names to generic names. The City, State, and Zip Code on all addresses will be changed to one common location different from the original. All social security numbers, driver's license numbers, bank account numbers, phone numbers, and tax ID numbers will be changed to meaningless strings of numbers. Any other data that is considered private or confidential will be changed to meaningless strings of characters.

Rare situations may arise that require an LGC employee to load a customer's data without scrambling the confidential data. If this occurs the employee must ask their manager or director to e-mail the designated department a request to load the database without scrambling the confidential data. The designated department will keep a log of the unscrambled databases. Use of unscrambled data will be limited to three workdays. At the end of the three-day period, the designated department will check with the LGC employee to make sure the unscrambled database has been removed. If the database needs to remain unscrambled for more time, an additional three-day period will be granted and the above procedure will be followed a second time.



Recommended Customer Actions

LGC also recommends that their customers follow these procedures and or implement these policies:

1. Establish an acceptable use policy for their office outlining practices and procedures for staff regarding identifying sensitive information.
2. Do not use email to send files with sensitive data like social security numbers, bank account numbers, etc. If this must be done, work with the recipient and utilize the encryption method they use. Password protection on these files is also recommended.
3. If data or sensitive files need to be transmitted to financial institutions, utilize their secure internet connection method.
4. Establish an approved email solution in your office that doesn't utilize web mail providers such as Yahoo, Hotmail, and Gmail.
5. All customers should put Internet security and proper use as a priority. Many security attacks begin as innocent email whose attachments may render your information insecure.

Resources

Software Security

- [AVG Anti-Virus](#) (virus protection)
- [SpyBot](#) (malware eradicator)
- [AdAware](#) (malware eradicator)
- [Malwarebytes](#) (malware eradicator)
- [AxCrypt](#) (file encryption)

FACTA Resources

- [Federal Trade Commission](#)
- [Model ID Theft Policy, Josh Jones, MTAS](#)

Other Resources

- [Official Consumer Credit Reporting Agency Opt Out credit site](#) - phone 1-888-567-8688
- [FTC ID Theft site](#)

Files included on LGC Website

- [FACTA - \(Actual Law\).pdf](#)
- [FACTA - Rules & Regulations.pdf](#)
- [Financial and Banking Information Infrastructure Committee \(FBIIC\) Internet Findings.pdf](#)
- [FTC delaying enforcement of FACTA compliance to May 2009.pdf](#)
- [FTC ID theft brochure.pdf](#)
- [FTC Take Charge.pdf](#)



Identified Sensitive Information

The information contained here is subject to change without notice.

- **W2 Diskette** – SSN, name, address, wage information
Required to be transmitted through the IRS website
- **1099 Diskette** – Vendor employer identification number (may be SSN), address, pay information
- **ACH Utility Billing Diskette** – Name, Banking Information, Account Number, Amount Billed
- **US Able Reporting File** – Payroll number, SSN, Address, Deduction information
For those using it from American Fidelity, they require the customer to upload the file to a secure FTP site.
- **Siesta Staff File** – Name, SSN, Address, Classification, Hire Date, Terminated date and other related substitute teacher information
- **American Fidelity** (new option coming soon)
- **Voter Daily File** – SSN, Name, other voter information
Transmitted through state website
- **Voter Public Files** (– Varies according to sort - Option to suppress SSN when building the file
This file is given to the public at their request
- **ACH Payroll Direct Deposit Files** – Name, Banking information and other pay information
- **TCRS Files** - SSN, Name, other pay information regarding retirement
These are copied to media and mailed to the state.
- **Employment Security** – SSN, Name, Employment Security information
These are copied to media and mailed to the state.
- **BIS UTB files** - Account number, name, address, phone number, amount due and other payment information
File uploaded to the BIS FTP site .
- **BIS Property Tax files** - Receipt number, name address, property tax information
File uploaded to the BIS FTP site.
- **Mortgage Delinquent File** - Receipt number, parcel number, tax year, total tax amount, amount paid, date paid, city number (no name or address)
These files are copied to media and sent to the mortgage companies –For some mortgage companies, LGC pulls the file and emails it to them.



Local Government Corporation *Information Security*

- **State Delinquent File** - Receipt number, county number, map and parcel, tax year, county delinquent code, city delinquent code (no name or address)
These files are sent to the state on a diskette.
- **Data Extractor** – Zortec option that allows customer to select information, some of which is considered sensitive, to be extracted to files or reports.