
Identity Theft Prevention Program Compliance



Identity Theft Prevention Program

For

Lancaster County Water and Sewer District

1400 Pageland Hwy, Lancaster SC 29720

Drafted October 10, 2008, Revised on 1/03/2024

Employees that this concerns will be given a copy for their records.

Lancaster County Water and Sewer District (LCWSD) Identity Theft Prevention Program

This Program is threefold in its purpose: i) identification; ii) detection; and iii) response. It is designed to identify relevant Red Flags for customer accounts, and incorporate those Red Flags into its Program. Once the Red Flags are identified, this Program will make it easier to detect possible identity theft on new or existing accounts. Upon such detection, LCWSD can respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft of its customers. In accordance with applicable law, LCWSD will update the Program periodically, so that it reflects changes in risks to customers and to the safety and soundness of LCWSD and its systems from identity theft. The initial Program was adopted in June of 2009 and has been reviewed and updated annually since that time; however, given the increase in cyberattacks on utility systems in 2020 and 2021, management has determined the Program needs to be amended to make sure LCWSD stays in the forefront of identity theft protection.

Contact Information:

The Senior Management Official responsible for this program is:
Name & Title: Bradley H. Bucy, Manager

The Governing Body Commissioners are:

1. Gerald White (Chairman)
2. Alfred C. Steele (Vice Chairman)
3. Robert Barr (Secretary)
4. R.J. Clyburn (Commissioner)
5. James C. Deaton (Commissioner)
6. Larry Hammond (Commissioner)
7. Robert A. Harris (Commissioner)
8. Stephen White (Commissioner)
9. Michael G. Williams (Commissioner)

Risk Assessment

LCWSD has conducted an internal risk assessment to evaluate i) the types of accounts it offers or maintains; ii) the methods it provides to open each type of account; iii) the methods it provides customers to access their accounts; and iv) its previous experiences with identity theft to determine how at risk the current procedures are for identity theft. This risk assessment evaluated how new accounts were opened; how existing accounts are maintained; and the methods used to access account information. Using this information, LCWSD was able to identify red flags from the following categories that were indicative of the possibility of identity theft. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- ❑ The presentation of suspicious documents when opening a new account, including, but not limited to the following:
 - a. Documents provided for identification appear to have been altered or forged;

- b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
 - c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
 - d. Other information on the identification is not consistent with readily accessible information that is on file with LCWSD from prior or other accounts; or
 - e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- The presentation of suspicious personal identifying information when opening a new account, including but not limited to the following:
- a. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, i.e., there is a lack of correlation between the SSN range and date of birth;
 - b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by LCWSD. For example:
 - i. The address on an application is the same as the address provided on a fraudulent application; or
 - ii. The phone number on an application is the same as the number provided on a fraudulent application;
 - c. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by LCWSD. For example, the phone number is invalid, or is associated with a pager or answering service;
 - d. The SSN or EIN provided is the same as that submitted by other customers;
 - e. The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
 - f. Personal identifying information provided is not consistent with personal identifying information that is on file with LCWSD; or
 - g. The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- The unusual use of, or other suspicious activity related to, an existing account, including, but not limited to, the following:
- a. The customer fails to make the first payment or makes an initial payment but no subsequent payments;
 - b. A covered account is used in a manner that is not consistent with established patterns of activity on the account, i.e., nonpayment when there is no history of late or missed payments;
 - c. Mail sent to the customer is returned repeatedly as undeliverable although water and/or sewer usage continues in connection with the account;
 - d. LCWSD is notified that the customer is not receiving paper account statements; or
 - e. LCWSD is notified of unusual or excessive charges in connection with the customer's account.

- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with customer accounts, whether new or existing, at LCWSD.

Detection (Red Flags):

Having identified the above Red Flags, in connection with the opening of covered accounts and existing covered accounts, LCWSD shall endeavor to detect these Red Flags by reviewing all reports, alerts or warnings received from reporting agencies, or other third-party services, related to fraud or identity theft; obtaining identifying information about, and verifying the identity of, a person opening a new account; monitoring the accounts of existing customers, and verifying the validity of change of address requests, in the case of existing accounts.

Response

The response of LCWSD to the detection of any of the identified Red Flags LCWSD will be commensurate with the degree of risk posed. In determining an appropriate response, LCWSD staff and management will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by LCWSD, or any of its third party vendors, or notice that a customer has provided information related to an account to someone fraudulently claiming to represent LCWSD or to a fraudulent website. In all instances upon the detection of a Red Flag, that detection shall be reported immediately to the Senior Management Official, who shall then decide upon the appropriate response, which may include the following:

- (a) Monitoring an account for evidence of identity theft;
- (b) Contacting the customer;
- (c) In the case of a new account, seeking additional documentation prior to opening the account;
- (d) Changing any passwords, security codes, or other security devices that permit access to customer accounts;
- (e) Reopening an account with a new account number;
- (f) Not opening a new account;
- (g) Closing an existing account;
- (h) Not attempting to collect on an account;
- (i) Notifying law enforcement; or

(j) Determining that no response is warranted under the particular circumstances.

After evaluation by the Senior Management Official, upon determination that a customer has been or is suspected to have been a victim of identity theft, LCWSD shall contact the customer by telephone, followed by providing written notice via certified mail. The written notice shall include the type of identifying information involved in the identity theft, the date (if it can be discerned) on which the theft occurred; and the following telephone numbers the customer may call for further information and assistance:

Local Law Enforcement: Lancaster County Sheriff 803-283-3388;

Federal Trade Commission: (Toll Free) 877-438-4338 or www.identitytheft.gov

Credit Reporting Agencies:

- Equifax: (800) 685-1111; Equifax.com/personal/credit-report-services
- Experian: (800) 397-3742; Experian.com/help
- TransUnion: (888) 909-8872; TransUnion.com/credit-help

Updating the Program

LCWSD shall update the Program (including the Red Flags determined to be relevant) annually, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

- (a) The experiences of LCWSD with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft; and
- (d) Changes in the service provider arrangements of LCWSD.

Administering the Program

The Senior Management Official shall update the Board of Commissioners on the development, implementation, and any amendment to the Program at least once every fiscal year. In the event of a confirmed instance of identity theft, the Senior Management Official may utilize his discretion to notify the Board at its regularly scheduled meeting and update the Board with the steps taken in response.

In addition to the Senior Management Official, the Business Manager shall be responsible for the day-to-day implementation of the Program. Together with the Information Technology Director and Office Manager of LCWSD, the Business Manager shall develop an annual report

to be presented to the Senior Management Official, which addresses material matters related to the Program and evaluates issues such as: i) the effectiveness of the policies and procedures of LCWSD in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts; ii) service provider arrangements; iii) significant incidents involving identity theft (if any) and management's response; and iv) recommendations for material changes to the Program.

The Business Manager shall also be responsible for training staff, as necessary, to effectively implement the Program and for exercising appropriate and effective oversight of service provider arrangements to insure those providers have reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Personal Information Security Procedures:

Lancaster County Water and Sewer District adopts the following security procedures:


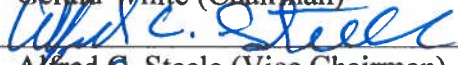

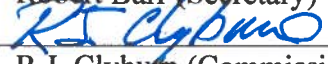
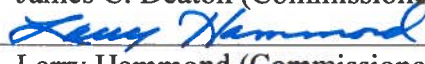

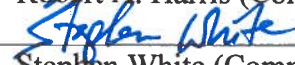
1. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
2. Employees log off or lock their computers when leaving their work areas.
3. No visitor will be given any entry codes or allowed unescorted access to the office.
4. The computer network will have a firewall where our network connects to the Internet.
5. Check references or do background checks before hiring employees who will have access to sensitive data.
6. Access to customer's personal identity information is limited to employees with a "need to know."
7. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop, tablet or smartphone.
8. Employees who violate security policy are subject to discipline up to, and including, dismissal.
9. Paper records that contain personal information will be shredded or incinerated before being placed into the trash receptacle.
10. Any data storage media will be disposed by shredding, punching holes in, or incineration.

11. Connecting non-LCWSD issued computers, laptops, pdas, cell phone or any other non-authorized device to Lancaster County Water and Sewer District's network is strictly prohibited.

12. Non-LCWSD employees shall not have access to any LCWSD issued laptops, pdas, cell phones or any other electronic device and LCWSD employees shall not allow such access.

This plan has been reviewed and adopted by the Commissioners of Lancaster County Water and Sewer District. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Signatures:

1.  Date 1/18/24
Gerald White (Chairman)
2.  Date 1/18/24
Alfred C. Steele (Vice Chairman)
3.  Date _____
Robert Barr (Secretary) Absent
4.  Date 1/18/24
R.J. Clyburn (Commissioner)
5. Absent Date _____
James C. Deaton (Commissioner)
6.  Date 1/18/24
Larry Hammond (Commissioner)
7.  Date 1/18/24
Robert A. Harris (Commissioner)
8.  Date 1/18/24
Stephen White (Commissioner)
9. Absent Date _____
Michael G. Williams (Commissioner)

For employees to sign

The signature below signifies that I have been given a copy and understand the importance of the Identity Theft Prevention Program.

Employee Signature

Printed Name

Date