

Red Flag Regulations

Executive Summary

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by May 1, 2009, and must provide for the identification, detection, and response to patterns, practices, or specific activities (red flags) that could indicate identity theft.

Under the Rules, Renewable Water Resources (ReWa) is responsible for developing a program as it falls under the category of having covered accounts. A covered account is a personal account that involves multiple payments or transactions such as credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. ReWa maintains utility accounts.

Some examples of covered accounts at ReWa are: Customer Service Accounts (Commercial and Residential), Customer Service Impact Fees, Manual Billings (Industrial, Commercial, and Residential), Industrial Accounts, and Septage Haulers. Currently six agencies, including Greenville Water System, bill for ReWa and eight agencies collect Customer Service Impact Fees for ReWa. Both ReWa and the agencies have access to the respective customer information. A letter has been sent to each of these agencies requesting a copy of their Red Flag Compliance Procedures.

Under the Red Flags Rules, ReWa must develop a written program that identifies and detects the relevant warning signs (red flags) of identity theft. These may include: unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The Red Flag program must also describe proper responses that would prevent and mitigate the crime and detail a plan for updates to the program. The program must be submitted to and approved by ReWa's Board of Directors. Once approved, ReWa's Red Flag Committee members, consisting of Barbara Wilson, Cathy Caldwell, Blake Visin, Patricia Dennis, and Stacey Green, must manage the program, provide staff training, and provide for oversight of any service providers.

Please see the attached Red Flag Rules program for Renewable Water Resources.

Western Carolina Regional Sewer
Authority dba Renewable Water
Resources (ReWa)

FACTA Section 114
Red Flag Plan

and

South Carolina Financial Identity
Fraud and Identity Theft Protection
Act

Protection of Consumer Information and Detection, Prevention and
Mitigation of Identity Theft for Covered Accounts

Adopted by the Board of Directors on *April 6, 2009*
[~~Insert Date~~]

Last Amended on [Insert Date]

WESTERN CAROLINA REGIONAL SEWER AUTHORITY
dba RENEWABLE WATER RESOURCES

RESOLUTION

RED FLAG PLAN

WHEREAS, the Federal Trade Commission issued regulations on November 9, 2007 requiring creditors that hold consumer accounts to develop and implement a written identity theft prevention program providing for the identification, detection and response to patterns, practices or specific activities known as "Red Flags" that could indicate identity theft; and

WHEREAS, the compliance with these "Red Flag" rules is required by May 1, 2009; and

WHEREAS, the General Assembly of the State of South Carolina approved the "Financial Identity Fraud and Theft Protection Act" (the "Act") on March 4, 2008, which was then subsequently ratified by the Governor on April 2, 2008; and

WHEREAS, the effective date of this Act is December 31, 2008, with the exception of certain provisions which are effective at different points in time following that date; and

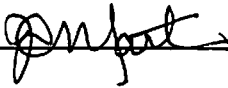
WHEREAS, the implementation of both the "Red Flag Rules" and the "Act" require Renewable Water Resources to establish policies limiting and managing the collection and dissemination of personal identifying and financial information, and the diligent pursuit of "red flags" which are indicators that identity theft is about to happen or has happened in the past in relation to our covered accounts;

NOW, THEREFORE, IT IS RESOLVED that:

1. The attached "Identity Theft Prevention Policy" (the "Policy") is hereby adopted with an effective date of May 1, 2009.

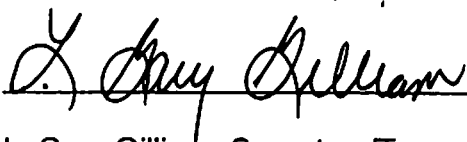
2. The Executive Director is hereby authorized to make changes to this policy as necessary to achieve and maintain compliance with the letter and the spirit of these requirements.

SIGNED AND SEALED this 6th day of April, 2009.



J.D. Martin, Chairman

ATTEST:



L. Gary Gilliam, Secretary/Treasurer

Designation of Committee(s)

1. RED FLAG IMPLEMENTATION COMMITTEE

This group is charged with the responsibility of performing the initial gap analysis, prioritizing deficiencies, performing market studies on solutions available, selecting and contracting for specific solution components, developing specific solution requirements, delivering training appropriate to deploy and maintain solutions, and documenting all of the above in the written Red Flag Prevention Program document to be submitted to the Board of Directors.

Cathy Caldwell

Stacey Green

Barbara Wilson

2. RED FLAG OVERSIGHT COMMITTEE

The members of this committee are charged with the daily responsibility of keeping the Program up to date and in compliance with FACTA Section 114 requirements. This committee will report to the Board on at least an annual basis to prove the effectiveness of the Program on the Covered Accounts and to make recommendations for any material changes to the Plan.

Cathy Caldwell

Stacey Green

Blake Visin

Patricia Dennis

Part 1: Risk Assessment

The Red Flag committee comprised of the Director of Human Resources, Director of Information Systems, Customer Service and Contract Manager, Controller, and the Administrative Finance Director has conducted a Risk Assessment, based on the requirements of FACTA, Section 114, and has determined that there is a need to implement a Red Flag Program for our organization. As such, we assessed which accounts must be included, based on the definitions for “covered accounts” as shown below.

Definition of a “Covered Account”

A “covered account” is a personal account that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.

A “covered account” is also any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

During our risk assessment we considered the following:

- The methods we provide to open our accounts;
- The methods we provide to access our accounts; and
- Our previous experiences with identity theft.

Under the definition of “Creditor” we also considered Covered Accounts as any account for which we provide a product or service and do not collect payment in advance or at the time of service, and any account where a consumer may default in payment after obtaining the product or service.

In addition we considered the potential for both new and existing account fraud based on the following threats that may result in the unauthorized access of personal information that can lead to identity theft:

- Technology intrusion (hacking, spyware, bots, etc.)
- Consumer deception (phishing, pharming, vishing, etc.)
- Employee theft of consumer information
- Social engineering – cons perpetrated against employees/customers
- Physical intrusion (break-in)
- Compromise of postal mail – both internal and at mailbox
- Loss/theft of laptop computers –unencrypted
- Other accidental loss – improper disposal of information, loss in transport, etc.

Based on the Risk Assessment we have determined that we will include, within the scope of our Red Flag Program, the following accounts or account categories:

Covered Accounts List:

1. Customer Service Accounts (Residential and Commercial)
2. Customer Service Impact Fees
3. Manual Billings (Industrial, Commercial and Residential)
4. Industrial Accounts
5. Septage Haulers

Part 2: Gap Analysis

Customer Service Accounts (Residential and Commercial)

Solutions in Place

A comparison of requirements of FACTA Section 114 and existing systems, policies, procedures and technologies indicates that some of the requirements have already been met, as indicated below.

Category	Solution	Description
Identity Verification <i>Knowing with a reasonable certainty that the identifying information that is presented to establish a new relationship is valid</i>	Yes	<ol style="list-style-type: none"> 1. Subdistricts establish new relationships with customers. ReWa does not establish this type of relationship. ReWa has requested Red Flag Procedures from Subdistricts who handle our customers. 2. Employees are assigned a unique name and password to log into the Customer Information System. This information is tracked by GWS and can be viewed on the Customer Information System. 3. We require customers calling in to state their unique identifying account and customer number, name, and address.
Identity Authentication <i>Knowing with a reasonable certainty the person presenting the identifying information is the owner of such information at the point of establishing a new relationship</i>	Yes	<ol style="list-style-type: none"> 1. Subdistricts establish new relationships with customers. ReWa does not establish this type of relationship. ReWa has requested Red Flag Procedures from Subdistricts who handle our customers. 2. We require customers calling in to state their unique identifying account and customer number, name, and address.

<p>Fraud Monitoring in Existing Accounts</p> <p><i>Proactive measures to identify patterns, practices or other indicators that identity theft is about to happen, is occurring or has happened in connection with our Covered Accounts</i></p>	<p>Yes</p>	<ol style="list-style-type: none"> 1. ReWa has requested Red Flag Procedures from Subdistricts who handle our customers. 2. Employees keep a log book of calls.
<p>Identity Theft Education for Employees</p> <p><i>Recognizing risk factors and methods to protect personal information in order to prevent identity theft</i></p>	<p>Yes</p>	<p>Training to come April 2009</p>
<p>Identity Theft Recovery Services for Mitigation of Risk and Damage</p> <p><i>A fraud department or outsourced professional Identity Theft Recovery Service to assist individuals who can not be validated for services or who are the subject of a Red Flag</i></p>	<p>Yes</p>	<p>If identity theft should occur, Renewable Water Resources will outsource as needed.</p>

Part 2: Gap Analysis

Customer Service Impact Fees

Solutions in Place

A comparison of requirements of FACTA Section 114 and existing systems, policies, procedures and technologies indicates that some of the requirements have already been met, as indicated below.

Category	Solution	Description
Identity Verification <i>Knowing with a reasonable certainty that the identifying information that is presented to establish a new relationship is valid</i>	Yes	Renewable Water Resources requires a tax map number, developer and subdivision name, and address to issue a permit for a new connection. If a customer pays for a new account fee by check, picture ID is required.
Identity Authentication <i>Knowing with a reasonable certainty the person presenting the identifying information is the owner of such information at the point of establishing a new relationship</i>	Yes	All information given is verified through Greenville County Real Property website or other County property search site. If a customer pays for a new account fee by check, picture ID is required.
Fraud Monitoring in Existing Accounts <i>Proactive measures to identify patterns, practices or other indicators that identity theft is about to happen, is occurring or has happened in connection with our Covered Accounts</i>	Yes	Employees keep an excel spreadsheet and access database of all new account fees paid. Accounting department also keeps record of fees paid.

<p>Identity Theft Education for Employees</p> <p><i>Recognizing risk factors and methods to protect personal information in order to prevent identity theft</i></p>	<p>Yes</p>	<p>Training to come in April 2009.</p>
<p>Identity Theft Recovery Services for Mitigation of Risk and Damage</p> <p><i>A fraud department or outsourced professional Identity Theft Recovery Service to assist individuals who can not be validated for services or who are the subject of a Red Flag</i></p>	<p>Yes</p>	<p>If identity theft should occur, Renewable Water Resources will outsource as needed.</p>

Part 2: Gap Analysis

Manual Billings (Industrial, Commercial and Residential)

Solutions in Place

A comparison of requirements of FACTA Section 114 and existing systems, policies, procedures and technologies indicates that some of the requirements have already been met, as indicated below.

Category	Solution	Description
Identity Verification <i>Knowing with a reasonable certainty that the identifying information that is presented to establish a new relationship is valid</i>	Yes	Renewable Water Resources requires name and address in person or by phone to open and access an account. Going forward new customers must present drivers license to validate address.
Identity Authentication <i>Knowing with a reasonable certainty the person presenting the identifying information is the owner of such information at the point of establishing a new relationship</i>	Yes	Renewable Water Resources requires business or company name and representative name and address in person or by phone to open and access an account. Going forward new customers must present drivers license to validate address.

<p>Fraud Monitoring in Existing Accounts</p> <p><i>Proactive measures to identify patterns, practices or other indicators that identity theft is about to happen, is occurring or has happened in connection with our Covered Accounts</i></p>	<p>Yes</p>	<p>Signatures will be required when activating new accounts in the future.</p>
<p>Identity Theft Education for Employees</p> <p><i>Recognizing risk factors and methods to protect personal information in order to prevent identity theft</i></p>	<p>Yes</p>	<p>Training to come in April 2009</p>
<p>Identity Theft Recovery Services for Mitigation of Risk and Damage</p> <p><i>A fraud department or outsourced professional Identity Theft Recovery Service to assist individuals who can not be validated for services or who are the subject of a Red Flag</i></p>	<p>Yes</p>	<p>If identity theft should occur, Renewable Water Resources will outsource as needed.</p>

Part 2: Gap Analysis

Industrial Accounts

Solutions in Place

A comparison of requirements of FACTA Section 114 and existing systems, policies, procedures and technologies indicates that some of the requirements have already been met, as indicated below.

Category	Solution	Description
Identity Verification <i>Knowing with a reasonable certainty that the identifying information that is presented to establish a new relationship is valid</i>	Yes	Renewable Water Resources requires that name of business and business representative, phone number, address and signature be attained before account is opened. Account number, name and address, and signature are required to gain access to accounts.
Identity Authentication <i>Knowing with a reasonable certainty the person presenting the identifying information is the owner of such information at the point of establishing a new relationship</i>	Yes	Collected information is verified by phone calls and on site visits.
Fraud Monitoring in Existing Accounts <i>Proactive measures to identify patterns, practices or other indicators that identity theft is about to happen, is occurring or has happened in connection with our Covered Accounts</i>	Yes	Log books will be kept to verify when access was granted.

<p>Identity Theft Education for Employees</p> <p><i>Recognizing risk factors and methods to protect personal information in order to prevent identity theft</i></p>	<p>Yes</p>	<p>Training to come in April 2009.</p>
<p>Identity Theft Recovery Services for Mitigation of Risk and Damage</p> <p><i>A fraud department or outsourced professional Identity Theft Recovery Service to assist individuals who can not be validated for services or who are the subject of a Red Flag</i></p>	<p>Yes</p>	<p>If identity theft should occur, Renewable Water Resources will outsource as needed.</p>

Part 2: Gap Analysis

Septage Haulers

Solutions in Place

A comparison of requirements of FACTA Section 114 and existing systems, policies, procedures and technologies indicates that some of the requirements have already been met, as indicated below.

Category	Solution	Description
Identity Verification <i>Knowing with a reasonable certainty that the identifying information that is presented to establish a new relationship is valid</i>	Yes	Renewable Water Resources requires that name, phone number, address and signature be attained before account is opened. Account number, name and address, and signature are required to gain access to accounts.
Identity Authentication <i>Knowing with a reasonable certainty the person presenting the identifying information is the owner of such information at the point of establishing a new relationship</i>	Yes	Collected information is verified by phone calls and on site visits
Fraud Monitoring in Existing Accounts <i>Proactive measures to identify patterns, practices or other indicators that identity theft is about to happen, is occurring or has happened in connection with our Covered Accounts</i>	Yes	Log books are kept to record accounts.

<p>Identity Theft Education for Employees</p> <p><i>Recognizing risk factors and methods to protect personal information in order to prevent identity theft</i></p>	<p>Yes</p>	<p>Training to come April 2009.</p>
<p>Identity Theft Recovery Services for Mitigation of Risk and Damage</p> <p><i>A fraud department or outsourced professional Identity Theft Recovery Service to assist individuals who can not be validated for services or who are the subject of a Red Flag</i></p>	<p>Yes</p>	<p>If identity theft should occur, Renewable Water Resources will outsource as needed.</p>

Part 3: List of Red Flags

Red Flags Listed in Subpart J, Appendix A

Following is a list of the Red Flags shown in FACTA Section 114, Subpart J, Appendix A, and an indication of “Applicable” if this Red Flag will be included in our Red Flag Program and “Not Applicable” if the Red Flag will NOT be included as part of this Red Flag Plan, and our reason for excluding the sample Red Flag.

Category: Alerts, Notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

1. A fraud alert or active duty alert is encountered on a credit file

N/A ReWa does not run credit reports

2. A consumer reporting agency provides a notice of a credit freeze in relation to a request for new credit, validation of existing credit or a new account

N/A ReWa does not utilize consumer-reporting agencies

3. A consumer reporting agency provides a notice of address discrepancy if such discrepancy that informs you that a substantial difference exists between the address for the consumer that you provided to request a consumer report and the address in the agency’s file for the consumer.

N/A ReWa does not utilize consumer-reporting agencies

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

- a) a recent and significant increase in volume of credit inquiries indicating requests for credit under the consumer’s name
- b) an unusual number of recently established credit relationships
- c) a material change in the use of credit, especially with respect to recently established credit relationships.
- d) credit accounts that were closed for cause or identified for abuse of account privileges by a financial institution or creditor

N/A ReWa does not utilize consumer-reporting agencies

Category: The Presentation of Suspicious Documents

5. Identifying documents presented by a consumer appear to have been altered or forged.

Applicable

6. A photograph or description of physical appearance on an identifying document does not match the applicant or customer presenting the identification.

Applicable ReWa asks for driver's license if a personal check is presented to pay a ReWa Impact Fee

7. Other information on the identification is not consistent with information provided by the person opening the new covered account or customer presenting the identification.

Applicable

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution, including signature cards, or recent checks.

N/A ReWa does not maintain copies of checks

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Applicable

Category: Suspicious Personal Identifying Information

10. Personal identifying information is inconsistent when compared against external data sources, such as a credit bureau or an identity validation service.
 - a) The address provided by the customer does not match any address in the consumer report, and/or
 - b) The SSN has not been issued or is listed in on the Social Security Administration's Death Master List

N/A ReWa does not use third party services

11. The date of birth and SSN do not correlate (i.e. based on the number it is possible to know approximately when the number was issued. If this does not correlate with the date of birth then additional validation may be required)

N/A ReWa does not use third party services

12. The address, SSN, telephone number or other piece of identifying information is consistent with information used in a fraudulent account, application or transaction, as reported to you by a third party service.

N/A ReWa does not use third party services

13. The address on an application is fictitious, a mail drop, or prison; or the phone number is invalid or associated with a pager or answering service as reported to you by a third party service.

Applicable for Industrial Billings, N/A for other account categories as ReWa does not validate with a third party service

14. The SSN provided is the same as that submitted by other persons that you have on file for a different customer or the same as other persons as reported to you by a third party service.

N/A ReWa does not obtain SSN or use third party services

15. The telephone number or address has been used by a large number of customers or other persons opening accounts as reported to you by a third party service.

N/A ReWa does not use third party services

16. The person opening the covered account or an existing customer fails to provide all required identifying information on an application or in response to a request for information to complete an application.

Applicable to manual and Industrial billing, N/A for Customer Service as billed by third party sources

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution.

N/A ReWa validates on suspicious documents only

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer can not provide authenticating information beyond that information that is typically found in a wallet or from public data.

N/A ReWa does not use questioning practices

Category: Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional or replacement cards or cell phone, or for the addition of authorized users on the account.

N/A ReWa does not receive such requests

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud.
- a. The majority of available credit is used for cash advances or merchandise that can be easily convertible to cash (ie. electronics equipment or jewelry)
 - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments

N/A ReWa does not offer revolving credit cards

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account.
- a) Non-payment when there is no history of late or missed payment
 - b) A material increase in the use of available credit
 - c) A material change in purchasing or spending patterns
 - d) A material change in electronic fund transfer patterns in connection with a deposit account
 - e) A material change in telephone call patterns in connection with a cellular phone account

N/A ReWa does not monitor account activity

22. A covered account is used after being inactive for a significant period of time (example provided: 2 years), taking into consideration the type of account and expected usage patterns and other factors

N/A ReWa does not monitor account activity

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

Applicable to Manual and Industrial Billing, N/A for other accounts as billed by third party services

24. The financial institution or creditor is notified that the customer is not receiving paper account statements. Documented procedures for responding to a customer's report that they are not receiving their paper statements in the mail.

Applicable to Manual and Industrial billing, N/A for Customer Service as billed by third party sources, N/A for Impact Fees as paid up front

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Applicable

Category: Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft that may not be your customer, a law enforcement authority or any other person that you have opened or are maintaining a fraudulent account for a person engaged in identity theft.

Applicable

Other Red Flags

The list below represents Red Flags incorporated into this Plan based on the experience of our organization, the experience of other organizations subject to the Red Flag rules and the relevant methods of identity theft at large.

Category: Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

27. A customer or non-customer reports receiving a collections notice regarding a debt that they did not incur.
- Applicable
28. A customer or non-customer reports receiving a billing for a new credit relationship, utility account, cell phone account or other debt or transaction account that they did not request.
- Applicable
29. A customer reports receiving a notice that his personal information was lost in a security breach incident.
- Applicable
30. The financial institution or creditor has an incident that results in the loss of personal information of customers.
- Applicable
31. A customer or non-customer reports responding to a phishing email or providing personal information on a cloned website that appears to be that of the financial institution or creditor.
- Applicable
32. A customer reports responding to a phishing email or providing personal information on a cloned website that appears to be that of a government agency, an organization or other financial institution or creditor.
- Applicable

Part 4: Detection and Response to Red Flags

Red Flag Response Protocol

Listed on the following charts are the Red Flag Response Protocol, including a list of Red Flags adopted by the Program, how and where each will be detected and possible responses to each Red Flag.

Red Flag Response Protocol

RED FLAGS	Where Red Flag Might Occur	How it Will Be Detected	Possible Responses	Notifications
<p>The Presentation of Suspicious Documents</p>				
<p>Documents appear forged or altered</p>	<p>Impact Fee Payment Industrial Billing Setup</p>	<p>Manual inspection of documents presented</p>	<p>Inquiry to financial institution as to account validity when appropriate.</p> <p>Validate with another form of ID (address, tax map number, photo required for personal checks).</p> <p>Physical validation of address and phone number for Manual billings.</p> <p>Track red flag and the appropriate response.</p>	<p>Communicate to individual or financial institution as appropriate.</p>
<p>Photo or physical description does not match person presenting identification</p>	<p>Impact Fee Payment</p>	<p>Manual inspection of documents presented as compared to visual observation</p>	<p>Obtain identifying information to prove with a reasonable certainty that the identity is valid and the person belongs to the identity prior to accepting impact fee payment via personal check.</p> <p>Track red flag and the appropriate response.</p>	<p>Communicate to individual or financial institution as appropriate.</p>

<p>Other info on ID is not consistent with info from person presenting info for impact fee payment</p>	<p>Impact Fee Payment</p>	<p>Manual inspection and comparison of identifying documents presented</p>	<p>Obtain identifying information to prove with a reasonable certainty that the identity is valid and the person belongs to the identity prior to accepting impact fee payment via personal check.</p> <p>Track red flag and the appropriate response.</p>	<p>Communicate to individual or financial institution as appropriate.</p>
<p>Application appears altered, forged, or appears destroyed and reassembled</p>	<p>Impact Fee Payment Industrial Billing Setup</p>	<p>Manual inspection of application presented</p>	<p>Obtain identifying information to prove with a reasonable certainty that the identity is valid and the person belongs to the identity prior to accepting payment for impact fee or establishing a manual billing account.</p> <p>If identity can not be validated deny the account until validation can be obtained.</p> <p>Track red flag and the appropriate response.</p>	<p>Communicate to individual that additional information is needed to validate identity.</p> <p>Communicate to individual or financial institution as appropriate.</p>

Suspicious Personal Identifying Information				
The address is fictitious, a mail drop, or prison	Industrial Billings Setup	Physical inspection of site.	<p>Contact customer to validate the address originally provided.</p> <p>Deny industrial billing account until address discrepancy is resolved.</p> <p>Track red flag and the appropriate response.</p>	Communicate to individual that additional information is needed to validate address.
The person attempting to open the account can not or will not provide all required information	Impact Fee Payment Industrial Billings Setup	Manual inspection of application presented	<p>Require necessary information before accepting impact fee or opening account.</p> <p>Track red flag and the appropriate response.</p>	Communicate to individual that additional information is needed before accepting impact fee or opening account.

Unusual Use of, or Suspicious Activity Related to the Covered Account				
<p>Mail sent to the customer is returned undeliverable, although transactions on the account continue</p>	<p>Manual Billing</p>	<p>Manual review and research of returned mail.</p>	<p>Contact customer at phone number on file to validate that correct address is reflected in billing. If address discrepancy can not be resolved via telephone, then physically inspect.</p> <p>Track red flag and the appropriate response.</p>	<p>Contact the customer at previously supplied phone number or phone number provided by directory assistance to determine the reason for the address discrepancy.</p>
<p>The customer notifies the creditor that they are not receiving their paper account statements</p>	<p>Manual Billing</p>	<p>Determine if the address on file to which statements are mailed is correct.</p>	<p>Contact customer at phone number on file to validate that correct address is reflected in billing. If address discrepancy can not be resolved via telephone, then physically inspect.</p> <p>Track red flag and the appropriate response.</p>	<p>This is a customer-initiated Red Flag, so no customer notification is necessary.</p>
<p>The creditor is notified of unauthorized charges or transactions in connection with a customer's covered account</p>	<p>Customer Service Accounts Manual Billings</p>	<p>A law enforcement agency, Identify Advocate or the customer reports fraud on a covered account.</p>	<p>Research customer's account activity. If unable to resolve via system and supporting document review, then physically inspect.</p> <p>Track red flag and the appropriate response.</p>	<p>Contact the customer after research performed to explain charges and handle any adjustments necessary.</p>

Reported Identity Theft or Identity Compromise				
The creditor is notified by a customer, a victim of identity theft that may not be our customer, a law enforcement authority or any other person that we have opened or are maintaining a fraudulent account for a person engaged in identity theft	Customer Service Accounts Impact Fees Industrial Billings Manual Billings	Notification by another financial organization, a law enforcement agency, a consumer who is a victim of identity theft, an Identity Recovery Advocate working under a LPOA for a victim or your customer.	Contact customer and law enforcement agencies as appropriate. Track red flag and the appropriate response.	Contact customer and law enforcement agencies as appropriate.
A customer reports receiving a collections notice regarding a debt that they did not incur.	Customer Service Accounts Manual Billings	Notification from the customer or an Identity Recovery Advocate working under a LPOA for an identity theft victim.	Research the customer's account activity. Track red flag and the appropriate response.	Contact customer and law enforcement agencies as appropriate.
A customer reports receiving a billing for a new utility account that they did not request.	Customer Service Accounts Manual Billings	Notification from the customer or an Identity Recovery Advocate working under a LPOA for an identity theft victim.	Research the customer's account activity. Track red flag and the appropriate response.	Contact customer and law enforcement agencies as appropriate.

<p>The creditor has an incident that results in the loss of personal information of customers. Each person whose information was compromised is at a higher risk.</p>	<p>Corporate Leadership Information Technology Security</p>	<p>Discovery of an organizational information security breach event could occur from several potential sources. Internally it could be discovered by IT, Pretreatment, Customer Service or the Finance Department. Externally it could be reported by a customer, a non-customer, law enforcement, or an Advocate working on behalf of an Identity Theft victim.</p>	<p>Activate Emergency Breach Response Plan as required by state law.</p>	<p>Notify customer via letter. Contact IDSafeResponse to address state breach requirements and risk mitigation.</p>
<p>A customer or non-customer reports responding to a phishing email or providing personal information on a cloned website that appears to be that of the creditor.</p>	<p>Customer Service Information Technology Security</p>	<p>Notification by a customer, a consumer who is not our customer or an Identity Recovery Advocate working under a LPOA for an identity theft victim.</p>	<p>If customer account information or personal identifying information is obtained through the phishing site, and this is a current customer, note on the customer's account and contact agency performing billing.</p> <p>Report phishing incident to the Federal Trade Commission or other consumer awareness organizations</p>	<p>Suggest to the customer that they contact one of the three major credit bureaus to place a fraud alert on their credit file.</p>

Part 5: Administration of the Red Flag Program

Periodic Risk Assessment

In accordance with the Administrative requirements of FACTA Section 114, we will perform a risk assessment on at least an annual basis to determine if we are correctly including the necessary accounts under our definition of Covered Accounts indicated in Part 1 of this Red Flag Plan Document. If we have excluded any accounts we will explain why we determined that there is no reasonable foreseeable risk to the consumer and to our organization from identity theft.

In addition, if we experience any of the following events within our organization we will conduct a new risk assessment as soon as practical in order to include any additional covered accounts.

1. Merger
2. Acquisition
3. Joint Venture
4. Alliance

Updating with New Red Flags

In accordance with FACTA, Section 114 we will update our Red Flag Program at least annually, if new Red Flags are identified based on the following considerations:

- **Our Experiences with ID Theft**
- **Changes in the methods of ID Theft at large**
- **Changes in methods to detect, prevent and mitigate ID Theft**
- **Changes in business arrangements, i.e. mergers, acquisitions, alliances, joint ventures, service providers, etc.**

Annual Report to the Board of Directors (or Senior Manager)

On at least an annual basis we will provide a report to the Board of Directors that will include the following:

Significant Incidents – a list of Red Flags found and any other significant identity theft/information breach issues that occurred within our organization or reported by our customers or employees.

Response to Significant Incidents – an indication of how each situation was handled and ultimately resolved.

Effectiveness on Covered Accounts – a summary of the effectiveness of the plan based on how the incidents above were handled.

Service Provider Oversight – a list of any new service providers and a description of the evaluation process conducted to assure compliance with Section 114 service provider oversight requirements.

Recommendations for Updating/Amending Program: - a recommendation for deletion, amendments or additions to the Red Flag Program.

Part 6: Compliance with the South Carolina Financial Identity Fraud and Identity Theft Protection Act

Overview:

The South Carolina General Assembly passed legislation on April 2, 2008 to address financial identity fraud and theft. This legislation requires businesses, as well as state and local governments, to protect social security numbers and other personal identifying information.

Consistent with federal laws the SC Financial Identity Fraud and Identity Theft Protection Act is intended to tackle the critical problem of identity theft by requiring entities collecting personal information to take steps to secure it. The Act also requires that leaked information be immediately disclosed to the consumer to prevent further loss.

ReWa will evaluate state legislation to ensure compliance with applicable laws.

Effective Dates:

Legislation passed on April 2, 2008. Sections 1,2,3,5, & 8 have an effective date of December 31, 2008; sections 4 & 7 have an effective date of July 1, 2009; and section 6 has an effective date of either December 31, 2009 or 2011 depending on the circumstances.

Part 7: Security of Electronic Records

General Network Security

- Computers which have connections to the computers where sensitive information is stored have been identified.
 - All the computers that have access to the GWS billing system.
 - All computers that have access to payroll system server.
- Sensitive consumer data will not be stored on any computer with an Internet connection unless it's essential for conducting business. Computers where Internet is not necessary for daily work, UBS ports should be closed.
- Sensitive information that is sent to third parties over public networks will be encrypted.
- Email transmissions will be encrypted if they contain personally identifying information.
- Anti-virus and anti-spyware programs will be run on individual computers and servers on a daily basis.
- Anti-virus and anti-spyware programs will be kept up-to-date.
- When sensitive financial information is received or transmitted, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

Password Management

- Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User name and password will be different. Passwords will be forced to change minimally every 90 days.
- Passwords will not be shared or posted near workstations.
- When new software is installed, vendor-supplied default passwords are immediately changed to a more "strong" secure password.

Laptop Security

Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on a laptop.

- The use of laptops is restricted to those employees whose jobs require one.
- Laptops are secured in a secure place and are only taken offsite when absolutely necessary. When necessary laptops are signed out by the employees.

- Employees are never to leave a laptop visible in a car, at a hotel room, or packed in checked luggage unless directed to do so by airport security.

Firewalls

- A firewall is used to protect all computers from hackers' attacks while it is connected to the Internet.
- "Access controls" settings are set to determine who gets through the firewall and what they will be allowed to see. This allows only trusted employees with a legitimate business need to access the network.
- Access controls will be reviewed periodically.

Wireless & Remote Access

- Limit employees who can use a wireless connection to access computer network. (This will make it harder for an intruder to access the network by limiting the wireless devices that can be hacked.)
- A transmission of sensitive information from a wireless device to a computer is encrypted. This may prevent an intruder from gaining access through a process called "spoofing"-impersonating one of the utilities computers to get access to the network.
- If remote access is allowed to a computer by employees or by service providers, information being transmitted is encrypted.
- ReWa's Wireless Access Points will not broadcast the Service ID.

Detecting Breaches

- An intrusion detection system is used to detect network breaches when they occur.
- The intrusion detection system is updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity, on networks so attacks can be spotted and responded to.
- Monitor incoming traffic for signs of a hacker trying to enter the system.
- Monitor outgoing traffic for signs of data breach. Watch for unexpectedly large amounts of data being transmitted from ReWa systems to an unknown user. If large amounts of information are being transmitted from the ReWa network, investigate to make sure the transmission is authorized.

Part 8: Employee Training

Train employees to spot security vulnerabilities. Periodic training emphasizes the importance of identifying security breaches. A well-trained ReWa workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Employees will sign a statement to follow ReWa confidentiality and security standards for handling sensitive data. This statement will be signed annually.
- Access to customer's personal identity information is limited to ReWa employees with a "need to know."
- Procedure is in place and followed for ReWa employees who resign or transfer to another department within the utility to no longer have access to sensitive information. Their passwords are terminated, key(s) collected and identification cards collected as part of the check-out routine.
- Regular scheduled employee training is held to update employees about new risk and vulnerabilities. Employees' attendance is mandatory
- ReWa employees are required to notify the Director of Information Systems and the Human Resources Director if there is a potential security breach, such as a lost or stolen laptop.
- ReWa employees who violate the security policy will be subject to disciplinary actions, up to and including termination.

Part 9: Security Practices or Contractors & Service Providers

- Before outsourcing any business functions – payroll, web hosting, data processing, etc. – the company’s data security practices will be compared to the utilities.
- Security issues for the type of data a service provider handles will be addressed in our contract with them.
- Service providers notify utility of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

Part 10: Disposal of Sensitive Information

Paper Records

- Paper records will be shredded before being placed into the trash. An outside shredding vendor may be used to shred large quantities of data with proper documentation of the shredding process.
- Paper shredders are available in the Administration Building and the Lab Ops Building.

Hardware Sanitation Procedures for Red Flag Compliance

When hardware is moved into surplus (disposal off site in any manner), the following hardware and procedures are enacted:

- Smart phones
 - The device is scrapped for usual equipment (antenna, battery, screen, carrying case) and the balance is destroyed on-site via a 20 ton press.
- Hand held devices (Treo, Palm, PDAs, etc.)
 - The device is scrapped for usual equipment (battery, screen, carrying case) and the balance is destroyed on-site via a 20 ton press.
- Copy Machines with scanning capabilities (third party maintenance and support)
 - The third party support for the Sharp copier/scanner has set the unit to immediately purge all scanned images. No documents are written to the hard drive in the unit.
- Fax Machines
 - All of our fax machines have static ram with no hard drive, therefore any image faxed is temporary with no residual copy stored.
- Flash Drives
 - Flash drives, due to their unsecured nature, are not issued as company policy. Their use is on a personal level, with the user being responsible for encryption and password protection of files on these devices or the device itself.
- Hard drives
 - Servers
 - All hard drives are removed from a decommissioned server and destroyed on-site via a 20 ton press
 - Workstations
 - All hard drives are removed from decommissioned workstations and destroyed on-site via a 20 ton press.
- Backup media (Magnetic or optical)
 - Destroyed

When hardware is repurposed (recycled within the agency), the following hardware and procedures are enacted:

- Smart phones
 - The device is reset/reformatted with a new identity for the receiving user.
- Hand held devices (Treo, Palm, PDAs, etc.)
 - The device is reset/reformatted with a new identity for the receiving user.
- Copy Machines with scanning capabilities
 - The third party support for the Sharp copier/scanner has set the unit to immediately purge all scanned images. No documents are written to the hard drive in the unit.
- Fax Machines
 - All of our fax machines have static ram with no hard drive, therefore any image faxed is temporary with no residual copy stored.
- Flash Drives
 - Flash drives, due to their unsecured nature, are not issued as company policy. Their use is on a personal level, with the user being responsible for encryption and password protection of files on these devices or the device itself.
- Hard drives
 - Servers
 - All hard drives are fdisked and reformatted with a new Operating System and placed within the agency in their new role.
 - Workstations
 - All hard drives are fdisked and reformatted with a new Operating System and placed within the agency in their new role.
 - Exceptions include the HR Manager and HR Director, where the hard drives are either destroyed or given back to these individuals.
- Backup media (Magnetic or optical)
 - Reformatted prior to reuse.
 - Exception is HR tapes (Payroll) which are never recycled.

Part 11: Secure Internet Transactions

On the external (internet) corporate website, two forms require the transmitting of either SS number or private corporate information. These include a prospective employee application and a new vendor application.

Our internet web server is dedicated to our agency only. No other agency or company, public or private, uses this server in any manner.

In addition, both forms referenced above utilize a secure server, using GeoTrust's certified 1024 bit encryption, and the transmission of both forms is from a secured server to a secured server; the forms are e-mailed via secure connection to specific recipients only. No data or database is stored or managed on the server.