BOARD OF GARRETT COUNTY COMMISSIONERS
ADMINISTRATIVE SESSION
March 26, 2013

IN ATTENDANCE

Chairman Robert G. Gatto
Commissioner Gregan T. Crawford
Commissioner James M. Raley

County Administrator R. Lamont Pagenhardt

1. The Board of County Commissioners met with Wendy Yoder, Director, Department of Financial Services and Nikki Brown, Accountant, Department of Financial Services, to discuss the County Identity Theft Prevention Program. Ms. Brown requested that the Program Policy be amended to add Adventure Sports Center International and to modify other department official names to reflect applicable designation. The Board, on a motion by Commissioner Crawford, seconded by Commissioner Raley, and made unanimous by Chairman Gatto approved the program amendments as presented on this date. The update is attached to these Administrative Session Meeting Minutes as Exhibit 1.

2. Commissioner Raley briefed the Board of County Commissioners and Mr. Pagenhardt on plans to proceed with operation of the Yough Overlook Visitor's Center. Ms. Yoder was in attendance for this session. Commissioner Raley had been working with State Highway Administration and Chamber of Commerce and the project is now projected to open on May 1st. The Chamber indicated they will begin the search for personnel for the facility and the County will develop a memorandum of understanding with the Chamber for staffing. Continued dialog on this matter will continue.

3. The Board of County Commissioners authorized Chairman Gatto to execute a letter of support to the Internal Revenue Service at the solicitation of Blue Moon Rising relative to their 501 (c) (3) non-profit status.

4. The Board of County Commissioners agreed to resubmit Carl Bender as a member and Joseph Winters as alternate member for consideration on the Garrett County Property Tax Assessment Appeal Board. There is a requirement for a list of 3 nominees for each seat therefore the Board will send the names considered when the re-appointment of Member Sue Shockey was undertaken.

5. Michael Koch, Director, Department of Economic Development; Frank Shap, Assistant Director, Department of Economic Development; and Cynthia Sharon, Project Manager, Department of Economic Development presented a list of preliminary Appalachian Regional Commission projects for consideration. The Department will compile preliminary project descriptions for the Board to review and prioritize at a date to be determined.

6. The Board of County Commissioners reviewed and finalized an agenda of topics to present the Senator Barbara Mikulski during her visit to the County on March 27, 2013. These topics will include the following.

Broadband

ARRA Grant One MD
90% connectivity by 2014
Main trunk line finished connecting 44 community anchors - hospital, schools, etc.
Middle mile open to private providers
Last mile by us white space frequencies
First of its kind in Nation
ISP private public partnership
3000 homes identified
Facilitated by ARC monies
Broad band expansion in rural areas today equivalent to rural electrification in 1930 ‘s

2014

First time since 1989 when held in Garrett County
Largest in bound
Prague, Deep Creek, London
Good meetings with all representatives - office spoke of economic impact $20MM
Point person for federal issues, federal grants, Brand USA
Vision and Legacy 5/5/5
Flotilla across Maryland with Wounded Warriors
ARC Funding

Sequestration

57 layoffs for one month closing Head start for July
3 permanent layoffs end of weatherization program
GC had 100% school readiness and no disparity gaps bet low income participants
5% of dispersed monies in FY 13

SCIF at the incubator

NSA approved
Beyond blast zone offers low impact economic development with higher paying jobs

Hurricane Sandy

Didn't reach threshold for Federal relief
New Emergency Operating Center

Dove Center

Sequestration fund cut impact $20K
Numbers have been up

7. The Board of County Commissioners met with members of the County LEAN Committee who presented a review of the process and final recommendation on County Travel Policy. This session was conducted at the County Department of Technology and Communications Center. The Committee reviewed the process for a recommended Travel Policy. The Board will take this matter under advisement.

8. Mr. Pagenhardt reviewed a number of administrative and managerial issues under his jurisdiction and responsibility.

Attest:

_____
R. Lamont Pagenhardt,
County Administrator

_____
Date

By Order of the Board,

_____
Robert G. Gatto, Chairman
Board of County Commissioners

EXHIBIT 1

BOARD OF COUNTY COMMISSIONERS OF GARRETT COUNTY, MARYLAND IDENTITY THEFT PREVENTION PROGRAM

PURPOSE OF PROGRAM

Pursuant to federal law the Federal Trade Commission adopted Identity Theft Rules (Red Flags Rule) requiring the creation of certain policies relating to the detection, prevention and mitigation of identity theft.

The Federal Trade Commission regulations adopted as 16 CFR § 681.2 require creditors, as defined by 15 U.S.C. § 681(a)(5) to adopt red flag policies to detect, prevent and mitigate identity theft with respect to covered accounts. 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C. § 1691a, which defines a "creditor" as a person that extends, renews or continues credit, and defines "credit" in part as the right to purchase property or services and defer payment therefor. The Federal Trade Commission regulations include utility companies in the definition of creditor. The Board of County Commissioners of Garrett County, Maryland (County) is a creditor with respect to 16 CFR § 681.2 by virtue of providing utilities or by otherwise accepting payment for goods or services in arrears.

The Federal Trade Commission regulations define "covered account" in part as an account that a creditor offers or maintains for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions and specifies that a utility account is a covered account. The Federal Trade Commission regulations require each creditor to adopt an Identity Theft Prevention Program which will use red flags to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The County provides goods and services for which payment is made after the goods have been received or the services have been provided. Many of these customer accounts are covered accounts by virtue of being for household purposes and allowing for multiple payments or transactions.

Accordingly, the County has enacted this Identity Theft Prevention Program in compliance with federal law.

IDENTITY THEFT PREVENTION PROGRAM

1. Purpose.

The purpose of this Program is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent or at least mitigate identity theft.

2. Definitions.

For purposes of this Program, the following definitions shall apply:

(a) "County" means the Board of County Commissioners of Garrett County, Maryland.

(b) "Covered Account" means (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, 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; (ii) Any other account that the financial institution or creditor offers or maintains 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.

(c) "Credit" means the right granted by the creditor to a debtor to defer payment of debt, to incur debts and defer its payment or to purchase property or services and defer payment therefor.

(d) "Creditor' means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. "Creditor" includes utility and telecommunications companies.

(e) "Customer" means a person that has a covered account with the County.

(f) "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any -

(1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number; government passport number, employer or taxpayer identification number;
(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(3) Unique electronic identification number, address or routing code; or
(4) Telecommunication identifying information or access device (as defined in 18 U.S. C. 1029(e)).

(g) "Identity theft" means a fraud committed or attempted using identifying information of another person without authority.

(h) "Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

(i) "Notice of address discrepancy" means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(j) "Oversight Committee" means the Committee appointed by the County to oversee operation and compliance of the County's Identity Theft Prevention Program in accordance with the requirements of the Fair and Accurate Credit Transaction Act.

(k) "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(l) "Service provider" means a person that provides a service directly to the County.

3. Findings

(1) The County is a creditor pursuant to 16 CFR § 681.1 due to it offering and maintaining covered accounts for which payment is made in arrears.

(2) Covered accounts offered to customers for the provision of County services include Adventure Sports Center International (ASCI), Airport 2G4, Animal Shelter/Control, Facilities & Maintenance, Human Resources, Permits & Inspections, Planning, Zoning, and Licensing, Public Utilities, Roads, Solid Waste & Recycling, and Technology & Communications (DoTCom) accounts.

(3) The County has no known prior experience with identity theft related to covered accounts.

(4) The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts, and transferring such accounts have been identified as potential processes in which identity theft could occur.

(5) The County limits access to identifying information to those employees who are responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of a covered account. All written applications associated with the covered accounts are maintained in file cabinets. Information provided in the applications is entered directly into County's computer system and is accessible only to those employees in County offices responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of a covered account.

(6) The County has determined that there is low (if any) risk of identity theft occurring in the following ways:

a. Use by an applicant of another person's identifying information to establish a new covered account;
b. Use by another person of a previous customer's identifying information in an effort to have service restored in the previous customer's name;
c. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts;
d. Use of another person's credit card, bank account, or other method of payment by a customer desiring to restore such customer's covered account;
e. Use by a third party of a customer's identifying information obtained by overhearing conversations between the County and the customer during the customer's application for service process.

4. Process of Establishing a Covered Account.

(1) As a precondition to opening a covered account in the County, the County may request the applicant provide the County with identifying information of the customer which shall be in the form of a valid state or federal government issued identification card, such as a state issued driver's license, a state issued identification card, a U.S. government issued passport or visa, or a U.S. military identification card, all of which must contain a photograph of the customer. For customers who are not natural persons such as a trust, the customer's agent opening the account must provide a valid state or federal government issued identification card and proof of authority to act on behalf of the trust.

If an applicant's name has been changed through marriage, divorce, legal name change, or otherwise, verification of the name change must be provided before an applicant will be allowed to establish a new account or transfer an existing account in a name different from that appearing on the required state or federal government issued identification card.

(2) The County does not now use consumer credit reports. Should the County begin using consumer credit reports, each applicant shall also be required to provide any information necessary for the County to access the applicant's consumer credit report.

(3) County employees responsible for opening new accounts shall take reasonable precautions to insure that third parties are not attempting to view or hear identifying formation as it is being supplied by the applicant.

(4) An applicant's identifying information shall be entered directly into the County's computer systems and all written applications shall be placed in a filing cabinet accessible only to County employees.

(5) The County allows customers to create accounts online via the Garrett County Online Information Portal. Names, addresses, email addresses, passwords, security questions and answers and the last four digits of the customer's credit card number (if the customer requests for quicker payment access) are stored on a County system accessible only to authorized Information Technology and Finance Staff.

5. Access to Covered Account Information.

(1) Access to customer accounts shall be password protected and shall be limited to authorized County employees.

(2) Passwords shall be at least 5 characters in length. All passwords are stored using a one way encryption algorithm, as such, the stored passwords cannot be decrypted or viewed.

(3) Any unauthorized access to or other breach of customer accounts is to be reported immediately to his or her supervisor and to the Oversight Committee. Any and all actions that may mitigate identity theft such as changing passwords should be implemented.

(4) Identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to his or her supervisor and to the Oversight Committee.

(5) Names, addresses, email addresses, passwords, security questions and answers and the last four digits of the customer's credit card number (if the customer requests for quicker payment access) are stored on a County system accessible only to authorized Information Technology and Finance Staff.

6. Credit Card Payments.

(1) The County allows payments through the internet. When a customer accesses his or her account via the internet to process payment, the credit card information is sent via an encrypted connection to a third party which processes the payment.

(2) Names, addresses, email addresses, passwords, security questions and answers and the last four digits of the customer's credit card number (if the customer requests for quicker payment access) are stored on a County system accessible only to authorized Information Technology and Finance Staff.

7. Sources and Types of Red Flags

All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

(1) Alerts from consumer reporting agencies, fraud detection agencies or service providers (if a consumer credit report is used).
Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by a consumer reporting agency;
d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    i. A recent and significant increase in the volume of inquires;
    ii. An unusual number of recently established credit relationships;
    iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
    iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(2) Suspicious documents.

a. Documents provided for identification that appear to be 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 to the County;

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

(3) Suspicious identifying information.

a. Identifying information provided that is inconsistent when compared against external information sources used by the County. For example:
   i. The address does not match any address in the consumer report; or
   ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

b. Identifying information provided by the customer is not consistent with other identifying information provided by the customer. For example, there is a lack of correlation between the social security number range and date of birth.

c. Identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the County. 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.

d. Identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the County. For example:
   i. The address on the application is fictitious, a mail drop, or a prison; or
   ii. The phone number is invalid, or is associated with a pager or answering service.

e. The social security number provided is the same as that submitted by other persons opening an account or other customers.

f. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.

g. The person opening the covered account or the customer fails to provide all required identifying information on an application or in response to notification that the application is incomplete.

h. Identifying information provided is not consistent with identifying information that is on file with the County.

i. 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.

(4) Unusual use of, or suspicious activity related to, the covered account.

a. Shortly following the notice of a change of address for a covered account, the County receives a request for the addition of authorized users to the account.

b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
   i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   i. Nonpayment when there is no history of late or missed payments;

ii. A material change in the usage of services.

d. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

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

f. The County is notified that the customer is not receiving paper account statements.

g. The County is notified of unauthorized charges or transactions in connection with a customer's covered account.

(5) 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 County

a. The County is notified by a customer, a victim of identity theft, a law enforcement official, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

8. Prevention and Mitigation of Identity Theft.

(1) In the event that any County employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to his or her supervisor. If, the employee in his or her discretion deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to his/her supervisor, who may in his or her discretion determine that no further action is necessary. If the supervisor in his or her discretion determines that further action is necessary, a County employee shall perform one or more of the following responses, as determined to be appropriate by the supervisor:

a. Contact the customer;

b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:

i. Change any account numbers, passwords, security codes, or other security devices that permit access to an account; or

ii. Close the account;

c. Cease attempts to collect additional charges from the customer in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;

d. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or

e. Take other appropriate action to prevent or mitigate identity theft.

(2) In the event that any County employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests that identity theft or attempted identity theft is likely or probable. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to his/her supervisor. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to his/her supervisor, who may in his or her discretion determine that no further action is necessary. If the supervisor in his or her discretion determines that further action is necessary, a County employee shall perform one or more of the following responses, as determined to be appropriate by the supervisor:

a. Request additional identifying information from the applicant;
b. Deny the application for the new account;
c. Notify law enforcement of possible identity theft; or
d. Take other appropriate action to prevent or mitigate identity theft.

9. Updating the Program.

The Board of County Commissioners of Garrett County, Maryland shall annually review and, as deemed necessary update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the County and its covered accounts from identity theft. In doing so, the Board shall consider the following factors and exercise its discretion in amending the program:

a. The County's experiences with identity theft;
b. Updates in methods of identity theft;
c. Updates in customary methods used to detect, prevent, and mitigate identity theft;
d. Updates in the types of accounts that the County offers or maintains; and
e. Updates in service provider arrangements.

10. Program Administration.

(1) In accordance with specified guidelines, the Board of County Commissioners of Garrett County, Maryland has designated an Oversight Committee to ensure the Program's regulatory compliance. The Oversight Committee is responsible for, but not limited to:

a. The development and implementation of the Program;
b. Approval of the written Program;
c. Ensuring compliance with all Program requirements as stated in this policy;
d. Conducting a periodic review of all incidents involving one or more red flag events;
e. At least annually, reviewing staff reports regarding compliance with this policy and Red Flag events that occurred during the previous period.

(2) The Oversight Committee is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the Oversight Committee, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to the Board of County Commissioners of Garrett County.

(3) The Oversight Committee will report to the Board of County Commissioners of Garrett County, Maryland at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

a. The effectiveness of the policies and procedures of the County in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
b. Service provider arrangements;
c. Significant incidents involving identity theft and management's responses; and
d. Recommendations for material changes to the Program.

(4) The Oversight Committee is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The Oversight Committee shall exercise his or her discretion in determining the amount and substance of training necessary.

11. Outside Service Providers.

The County engages third party service providers to perform activities including billing distribution and online payment processing in connection with covered accounts. The Oversight Committee shall review such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures agreed upon by contract that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

12. Treatment of Address Discrepancies.

At the present time the County is not using consumer credit reports. If in the future the County begins to use consumer credit reports, the County will comply with federal regulations regarding treatment of address discrepancies. In the event that the County receives a notice of address discrepancy, the County employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

(1) Compare the information in the consumer report with:
   a. Information the County obtains and uses to verify a consumer's identity in accordance with the requirements for the Customer Information Program rules implementing 31 U.S.C. § 5318(1);
   b. Information the County maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or
   c. Information the County obtains from third-party sources that are deemed reliable by the relevant County employee; or

(2) Verify the information in the consumer report with the consumer.

13. Furnishing Consumer's Address to Consumer Reporting Agency.

(1) In the event that the County reasonably confirms that an address provided by a consumer to the County is accurate, the County is required to provide such address to the consumer reporting agency from which the County received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:

   a. The County is able to form a reasonable belief that the consumer report relates to the consumer about whom the County requested the report;
   b. The County establishes a continuing relation with the consumer; and
   c. The County regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.

(2) Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the city to such agency for the reporting period in which the city establishes a relationship with the consumer.

14. Methods of Confirming Consumer Addresses.

The County employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

   (1) Verifying the address with the consumer;
   (2) Reviewing County's records to verify the consumer's address;
   (3) Verifying the address through third party sources; or
   (4) Using other reasonable processes.