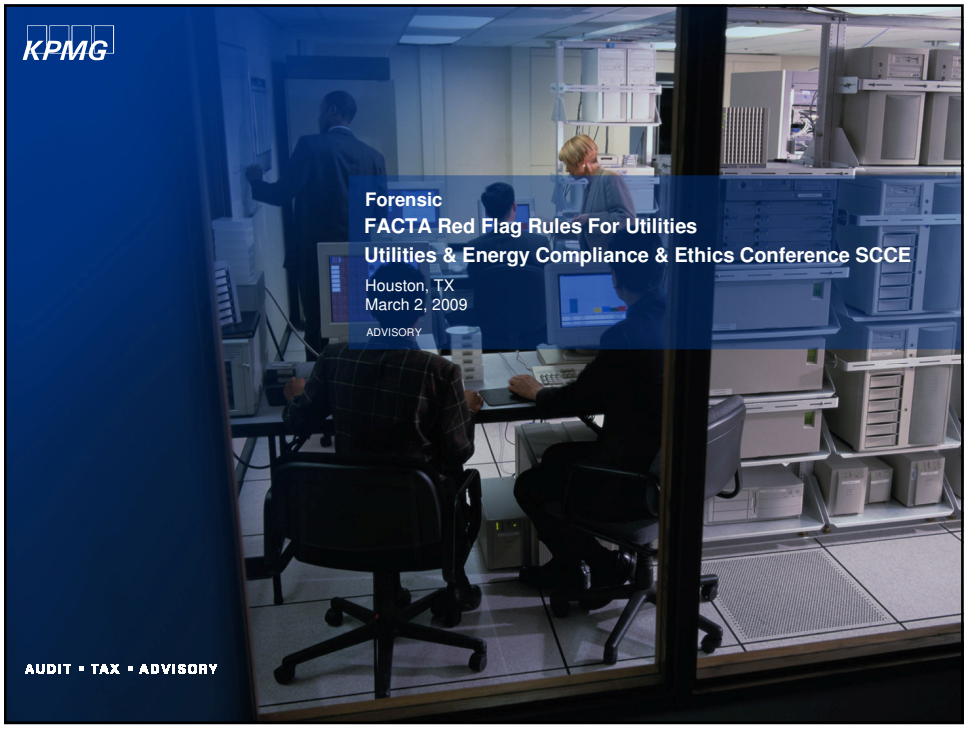

Agenda

1. Recent Information
2. Background on FACTA
3. Key Definitions
4. Applicability
5. Conducting the Risk Assessment
6. Address Discrepancies
7. Identity Theft Prevention Programs
8. Red Flags
9. Program Administration
10. Possible Steps to Take
11. Other Considerations

KPMG

1. Recent Information

The number of data security breaches in the United States "has reached an all-time high"*

- Reports of data breaches increased dramatically in 2008. The Identity Theft Resource Center's (ITRC) 2008 breach report reached 656 reported breaches at the end of 2008, reflecting an increase of 47% over 2007's total of 446.
- According to ITRC reports, only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It appears that the bulk of breached data was unprotected by either encryption or even passwords.

** (Source: Identity Theft Resource Center http://www.idtheftcenter.org)*

1. Recent Information (cont'd)

Government Data Breaches (select; 2008):

Date Made Public	Name/Location	Records Affected
12/15/2008	FEMA/Katrina	17,000
12/1/2008	NH Department of Health	9,300
10/30/2008	Agency for Workforce Innovation	250,000
10/30/2008	Jefferson County, WV	1,600,000
10/25/2008	NC DHHS	85,045
8/2/2008	TSA	33,000
Unknown	AZ Dept. Economic Security	40,000
Unknown	Texas Lottery	89,000
3/31/2008	U.S. Army	50,000
3/28/2008	CollegeInvest	200,000
1/8/2008	Wisconsin DHHS	260,000
	Total Selected Loss	**2,633,345 records**

(Source: Identity Theft Resource Center http://www.idtheftcenter.org)

1. Recent Information (cont'd)

Private Sector Data Breaches (select; 2008):

Date Made Public	Name/Location	Records Affected
12/15/2008	FEMA/Katrina	17,000
12/1/2008	NH Department of Health	9,300
10/30/2008	Agency for Workforce Innovation	250,000
10/30/2008	Jefferson County, WV	1,600,000
4/1/2008	Pfizer	13,000
2/27/2008	BNY Mellon Shareholder Services	12,500,000
	Total Selected Loss	**14,389,300 records**

(Source: Identity Theft Resource Center http://www.idtheftcenter.org)

1. Recent Information (cont'd)

- In November 2008, the Associated Press reported that in North Carolina, a man stole the identity of a three (3) year old and used the child's social security number to sign up for telephone and natural gas services. The theft was discovered when the grandmother of the child began receiving calls from a collection agency regarding unpaid utility bills in the child's name.

  (See, "Man accused of stealing 3-year-old's identity." The Associated Press State & Local Wire. November 25, 2008.)

- A man who lived in Seattle had his identity stolen and used to open up an account with the Puget Sound Energy Company and the Seattle City Light Department. The theft was discovered when he received a collection notice for an unpaid energy bill. The man also learned that the thief ran up a $2500 bill with the light department.

  (See, "Heckman, Candace. "Well Spent: ID theft can extend to utility fraud as well." Seattle PI.com. April 12, 2006.)

1. Recent Information (cont'd)

- The Identity Theft Resource Center (ITRC) released a report on the impact of identity theft victimization in 2008.
- The report outlined victims' responses to the use of their stolen personal information.
  - More than one-half (57%) of the respondents reported their personal information had been used to open a new line of credit in their name.
  - **Thirteen percent (13%) of the respondents indicated that their information was used to obtain new utility and/or cable services.**
  - According to this report, credit issuers, utility companies, and collection agencies rated poorly in their handling of identity theft victims.
  - This may draw attention of the regulators under the new rules.

(Source: Identity Theft Resource Center http://www.idtheftcenter.org)

2. Background on FACTA

- The Fair and Accurate Credit Transactions Act (FACTA) was signed into law in December 2003.
- In November 2007, the Federal Trade Commission (FTC) and the federal banking agencies jointly issued final rules under FACTA for the detection, prevention, and mitigation of identity theft.
- The original compliance deadline was November 1, 2008, and the banking agencies required adherence to that deadline.
- **The FTC has postponed enforcement until May 1, 2009.**

2. Background on FACTA (cont'd)

- Section **§114 (the Red Flag Rule)** requires
  - The development and implementation of a written Identity Theft Prevention Program (the Program) and applies to financial institutions and creditors that open or have existing covered accounts.
- Section **§315 (the Address Discrepancy Rule)** refers to resolution of credit report address discrepancies and applies to
  - Users of consumer credit reports
  - Persons requesting consumer credit reports from a Consumer Reporting Agency (CRA)

2. Background on FACTA (cont'd)

- The **Red Flag Rule (§114)** primarily requires creditors to:
  - **Develop** and implement a written Identity Theft Prevention Program (the Program)
  - **Train** "relevant" staff to implement the Program
  - **Report** at least annually to the board of directors, a committee thereof, or senior management on compliance with the regulations

2. Background on FACTA (cont'd)

- The **Address Discrepancy Rule (§115)** requires users of consumer credit reports to develop and implement reasonable policies and procedures that:
  - A. Enable the user to form a reasonable belief that a consumer credit report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.
  - B. Furnish an address for the consumer that the user has reasonably confirmed is accurate to the Consumer Reporting Agency (CRA), a clearinghouse for consumer credit history information, from which it received the notice of address discrepancy when the user:
    - Establishes a continuing relationship with the consumer
    - Furnishes information (regularly and in the ordinary course of business) to the CRA from which the notice of address discrepancy relating to the consumer was obtained

3. Key Definitions

Definitions We Will Cover:

1. Credit and Creditor
2. Covered Accounts
3. Identity Theft
4. Red Flags

3. Key Definitions (cont'd)

The Definition of "Credit" and "Creditor" from 15 U.S.C. § 1691a

- The term **"credit"** means
  - — the right granted by a creditor to a debtor to:
    - Defer payment of debt,
    - Incur debts and defer its payment, or
    - Purchase property or services and defer payment therefore.
- The term **"creditor"** means
  - — Any person who regularly:
    - Extends, renews, or continues credit,
    - 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.

3. Key Definitions (cont'd)

Covered Accounts

- The Red Flag Rule provides a two-part definition:
  1. "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."

     or

  2. "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."

3. Key Definitions (cont'd)

The FTC and the banking agencies' two-part definition of **identity theft** is:

A. "A fraud committed or attempted using the identifying information of another person without authority."

or

B. The creation of a fictitious identity using any single piece of information belonging to a real person because it involves "using the identifying information of another person without authority."

Therefore…

Identity theft applies to the use of identifying information of another person in opening new accounts, as well as the unauthorized use or "takeover" of an existing account.

3. Key Definitions (cont'd)

A "Red Flag" is defined in the regulations as:

"A pattern, practice, or specific activity that indicates the possible existence of identity theft."

- Red Flags are a crucial tool and are frequently implemented in a variety of ways as a key defense against fraud and use of stolen identities.
- Some are very specifically defined, while others may not be, but still serve as an indicator that something fraudulent or potentially fraudulent is occurring or is being attempted.
- Red Flags change over time and must be updated or revised to help ensure that they are working effectively for your organization.

4. Applicability

The FTC and the Agencies use a two-pronged approach to determine who is covered by this regulation:

- Covered entities
- Covered accounts

4. Applicability – Creditors

The first step for determining applicability is to determine if your organization is a creditor (utilities are generally considered to be creditors).

Covered Creditors

Those affected under the FTC section of the rules, based on the definition of "creditors", generally encompass:

- **Energy/Utility Companies**
- Municipalities
- Finance Companies
- Higher Education
- Medical Providers
- Automobile Dealers
- Telecommunications Companies

4. Applicability – Utility Companies

Utility companies are considered creditors because:

- Utilities bill customers after providing services, not before, and are extending a form of credit to the customer and intend to do so on a recurring basis.
- Utilities sometimes provide flat monthly payment plans (flex billing or equalized billing programs) that result in high credit balances for part of each service year.
- In the event of non-payment, utilities may enter into a payment plan or formal loan contract that is considered an extension of credit.

4. Applicability – Accounts

The second step for determining applicability is conducting the **risk assessment** to determine whether your organization a) offers or b) maintains covered accounts, specifically taking into consideration:

- Methods to open accounts
- Methods to access its accounts
- Previous experiences with identity theft and frauds related to stolen identities

Notes:

- The risk assessment must include subsidiaries, which are not separate entities, regardless of their location, and come under FACTA.
- This would include all of the subsidiaries of energy holding companies.
- The Red Flag Rule does not require single, non-continuing transactions to be covered.

4. Applicability – Accounts (cont'd)

As noted in the Federal Register, the FTC and the banking agencies also believe that small business accounts and/or sole proprietorship accounts may be vulnerable to identity theft, and, should therefore be considered by creditors for coverage under the Program.

- A creditor should consider whether there is a reasonably foreseeable risk of identity theft for business accounts it offers or maintains, especially those that may be opened or accessed remotely.
- Because of the risk-based nature of the rules, each creditor has the flexibility to determine which business accounts will be covered by its Program through its own risk evaluation process.

5. Conducting the Risk Assessment

When conducting the FACTA risk assessment, consider previous experiences with identity theft or stolen identity fraud, and focus attention on several key areas:

- Have customers, currently or historically, reported unusual or incorrect collection activity on their credit report for utility service they never received?
- Is the Company aware of specific instances where customers established service with an identity other than their own?
- Has the Company taken prior action in regard to an identity theft allegation or report by an identity theft victim?
- Has the Company been contacted by any law enforcement agency or regulatory body in response to an allegation of identity theft?

5. Conducting the Risk Assessment (cont'd)

Utilities should consider the following areas:

- Methods used to open accounts
- Methods used to access its accounts
- Previous experience with identity theft or similar frauds

5. Conducting the Risk Assessment (cont'd)

Utilities should consider the risks for all of the ways that a new account can be created:

- New accounts opened in person
- New accounts opened via telephone
- New accounts opened via fax
- New accounts opened via Web
- New accounts opened via mail

5. Conducting the Risk Assessment (cont'd)

When conducting the risk assessment around account creation, utilities may specifically focus attention on several key areas:

- What information is requested from the applicant?
- Is the information routinely verified via a CRA or other mechanism?
- Are there responses or forms of information presented by an applicant which may be considered suspicious from an identity theft perspective?
- What types of identification has the Company accepted in the past, and are those forms of ID currently accepted to establish accounts?
- Are Customer Service Representatives or Account Establishment Specialists trained in identifying Red Flags for the use of stolen identities?

5. Conducting the Risk Assessment (cont'd)

When conducting the risk assessment around account access, utilities may specifically focus attention on several key areas:

- How can customers access their accounts?
  - Via phone, Internet, fax, or mail
- When initiating changes to or releasing information regarding an existing customer account, what verification procedures are used?
- What is the success rate of controls in place to protect information breach, and have any information breaches, reported or unreported, occurred previously?

5. Conducting the Risk Assessment (cont'd)

A risk assessment may also be strengthened by evaluating current policies and procedures related to the Company's response to identity theft detection. When conducting this risk assessment, utilities may specifically focus attention on several key areas:

- What documents are acceptable for identity verification and what is the acceptable form of presentation (fax, e-mail, internet, personal presentation)?
- How do they authenticate documents before establishing service (call a landlord on a lease, etc.)?
- What is the Company's response mechanism for issues believe to be potential identity theft?
- What is the Company's flexibility in modifying or denying service to a perceived identity thief (depends highly on PUC/PSC regulations)?

5. Conducting the Risk Assessment (cont'd)

A risk assessment may also be strengthened by an analysis of the level of current training of account establishment personnel.

Important training components might include:

- How to identify suspicious documents when presented for identity verification
- How to respond to suspicious information provided in the application process
- How to respond to CRA information which may be indicative of identity theft
- How to respond to reports of identity theft by callers into the Company's call center
- How to monitor accounts for signs of identity theft

6. Address Discrepancies

The Address Discrepancy Rule (FACTA § 315 ~16 CFR § 681.1)

Businesses must have reasonable policies and procedures to deal with consumer reports that reflect an address discrepancy, in order to confirm that the report relates to the correct person.

- Compare the information in the consumer report with the following:
  - — Information developed in accordance with Customer Identification Program (CIP) guidance
  - — Information maintained in existing records, such as applications, change of address notifications, other customer account records, or retained documentation
  - — Information obtained from independent third-party sources

6. Address Discrepancies (cont'd)

Because many new utility customer applicants may be moving into the Company's service territory for the first time, an address discrepancy between the CRA and the applicant is not unusual.

Potential responses to address discrepancies may include:

- Request a state issued ID with the service address
- Request an account statement from another utility or service provider which can be verified
- Request a copy of a mortgage statement or lease
- Request a pay stub which shows the applicant's address
- Request a change of address statement from the United States Postal Service
- Request any additional information which the Company feels will establish the applicant does indeed reside at the address given

6. Address Discrepancies (cont'd)

- If your organization is unable to resolve an address discrepancy then:
  - It is expected that the consumer report will not be used, and
  - If your organization is not just a recipient, but also a provider of credit information, then the discrepancy should be reported back to the CRA.
- An address discrepancy may be a Red Flag to identity theft and may, therefore, require an appropriate response as defined within your Program.

7. Identity Theft Prevention Programs

Identity Theft Prevention Programs required by the Red Flag Rule (FACTA §114) must include reasonable policies and procedures to achieve the following four elements:

1. **Identify** relevant Red Flags for the covered accounts that the creditor offers or maintains, and incorporate those Red Flags into its Program
2. **Detect** Red Flags that have been incorporated into the Program of the creditor
3. **Respond** appropriately to any Red Flags that are detected to prevent and mitigate identity theft
4. **Update** the Program (including the Red Flags) periodically to reflect changes in risks to customers and/or to the safety and soundness of the creditor from identity theft

7. Identity Theft Prevention Programs (cont'd)

- Additional elements of the Program are:
  - Programs must be appropriate to the size and complexity of creditors and the nature and scope of their activities
  - Programs must incorporate oversight of third-party service providers to ensure regulatory compliance
  - Programs and risk assessments must be periodically updated
  - The Program may incorporate existing policies and procedures

7. Identity Theft Prevention Programs (cont'd)

- The e-commerce aspects of your Program should be considered. Many utilities open accounts over the phone and via the Internet.
- Online applications should undergo the same process of identity verification as telephone or in person applications for service.
- A creditor such as a utility may need to use non-documentary methods of customer verification.

7. Identity Theft Prevention Programs (cont'd)

Customer Verification

- Non-documentary verification methods may be needed in the following situations:
  - The customer opens the account without appearing in person
  - The account is opened without obtaining documents (e.g., the organization obtains the required information from the customer with the intent to verify it)
  - Customer is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard
  - The organization is not familiar with the documents presented

7. Identity Theft Prevention Programs (cont'd)

- Non-documentary methods of customer verification may include:
  - Contacting the customer
  - Checking references with other businesses or institutions
  - Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a CRA, public database, or other source
- Utilities can subscribe to services that provide information to assist with customer verification

8. Red Flags

The Program Must Include Relevant Red Flags

When identifying relevant Red Flags for covered accounts, a creditor should consider the following risk factors:

- The types of covered accounts offered or maintained
- The methods used to open covered accounts
- The methods used to access covered accounts
- Previous experience with identity theft

8. Red Flags (cont'd)

Sources of Red Flags

Creditors such as utilities should incorporate relevant Red Flags from various sources such as:

- Incidents of identity theft experienced by the utility or creditor
- Trade associations, Internet anti-fraud sites, and news resources
- Applicable supervisory guidance

8. Red Flags (cont'd)

The Regulation Identifies Five Categories of Red Flags and Provides at Least 26 Examples

The categories are:

- Alerts, Notifications, or Warnings from a Consumer Reporting Agency
- The Presentation of Suspicious Documents
- Suspicious Personal Identifying Information (PII)
- Unusual Use of, or Suspicious Activity related to a Covered Account
- Notifications or Reports from Consumers, Victims, Law Enforcement, or Others

8. Red Flags (cont'd)

Alerts, Notifications, or Warnings from a Consumer Reporting Agency

- Examples:
  - Fraud alerts or active duty notifications
  - Credit freeze notification
  - Address discrepancies
  - Inconsistent activity patterns

8. Red Flags (cont'd)

The Presentation of Suspicious Documents

- Examples:
  - Appearance of altered or forged documentation
  - Discrepancies between written descriptions and photographs of the customer
  - Inconsistency between information presented and what is on file

8. Red Flags (cont'd)

Suspicious Personal Identifying Information (PII)

- Examples:
  - Inconsistent with other PII or existing file information
  - Inconsistent with external sources
  - Associated with a different account in another name
  - Suspected or determined to be associated with fraudulent activity
  - Provided by a customer who is unable or unwilling to respond to advanced authentication questions

8. Red Flags (cont'd)

Unusual Use of, or Suspicious Activity Related to a Covered Account

- Examples:
  - — Numerous address changes in a short time frame
  - — Addition of new meters or service locations on the same account
  - — Activity commonly associated with fraud (i.e., terminated auto pay, refusal to pay deposit or first month's payment, returned checks, account in immediate arrears)
  - — Inconsistent account activity, to include non-payment after a history of on-time payments
  - — Notification of undeliverable mail relating to an account, especially when the account is active

8. Red Flags (cont'd)

Notifications or Reports from Consumers, Victims, Law Enforcement, or Others

- Examples:
  - — By a customer
  - — By a victim of identity theft
  - — By a law enforcement official or agency
  - — Any other person such as an employee who has opened an account they believe to be fraudulent for a customer potentially using a stolen identity

8. Red Flags (cont'd)

Detection of Red Flags

- The Program's policies and procedures should address the detection of Red Flags in connection with new and existing covered accounts by requiring:
  - — **Verification** of a person's identity
  - — **Authentication** of customers
  - — **Monitoring** of transactions
  - — **Validating** change-of-address requests

8. Red Flags (cont'd)

Response to Red Flags

- The Program's written policies and procedures should provide for appropriate responses to the Red Flags that are detected and are commensurate with the degree of risk posed
- In determining an appropriate response, a creditor should consider other factors that may heighten the risk of identity theft, such as:
  - — A data security incident

    or
  - — A notice related to a covered account, or associated with someone fraudulently claiming to represent the business or related to a fraudulent Web site

8. Red Flags (cont'd)

According to the rules, appropriate responses to mitigate identity theft may also include:

- Monitoring a covered account for evidence of identity theft
- Contacting the customer
- Changing passwords, security codes, or other security devices that permit access to a covered account
- Reopening a covered account with a new account number
- Not opening a new covered account*
- Closing an existing covered account*
- Notifying law enforcement

** There may be statutory restrictions related to these actions.*

9. Program Administration

Each creditor that is required to implement a Program must incorporate the following administration procedures:

- **Obtain approval** of the initial written Program from either the board of directors or an appropriate committee of the board of directors
- **Involve the board of directors**, an appropriate committee thereof, or a designated employee at the level of senior management in: oversight, development, implementation and administration of the Program
- **Exercise oversight** of third party service providers appropriate and ensure that they have implemented "reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft"
- **Train staff**, as necessary, to effectively implement and operate the Program
- **Report annually** to the board, a board committee, or a designated member of senior management

9. Program Administration (cont'd)

Program Updating

Programs (including the Red Flags) should be updated periodically to reflect changes in:

- Risks to customers
- Risks to the safety and soundness of the institution or creditor from identity theft, based on:
  - The experiences of the creditor with identity theft
  - Changes in methods of identity theft
  - Changes in methods to detect, prevent, and mitigate identity theft
  - Changes in the types of accounts offered or maintained
  - Changes in business arrangements of the creditor

9. Program Administration (cont'd)

Consider involving multiple business units in the development and administration of your Program. This may help to ensure that it is comprehensive, cohesive, effective, and efficient.

Business units which might be included:

- Compliance
- Legal
- Security/ Investigations
- Customer Service
- Information Technology
- Accounting/ Finance

10. Possible Steps to Take

- Review the rules in the Federal Register
- Determine if your organization is a covered entity within the meaning of the rules
- Develop, conduct, and document an enterprise-wide risk assessment to determine applicability of the rules to accounts offered and maintained.
- Develop and conduct a gap analysis of any existing programs, policies, and procedures
- Assess the Red Flags currently employed for appropriateness
- Evaluate Red Flag detection and monitoring systems, methodologies, results and response
- Draft a program and incorporate existing identity theft prevention and anti-fraud programs
- Have the board approve the written program
- Develop and deploy Red Flag training programs for relevant personnel
- Contact regulators to discuss exactly what they will be expecting after May 1, 2009

11. Other Considerations

- Potential Political Pressure(s)
- Regulatory Environment
- Economic Environment
- Examination Procedures

References

Federal Register

Vol. 72, No. 217, Nov. 9, 2007, (63718–63775)

http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf

FTC Press Release

http://www.ftc.gov/opa/2007/10/redflag.shtm

FTC Business Alert

http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

FTC Policy Statement

http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf

Contacts

Bryan O'Connell, CFE, CAMS
Manager – Advisory
KPMG LLP
99 High Street
Boston, MA 02110-2371
Tel: 617-988-1835
bryanoconnell@kpmg.com

Joseph P. Dooley, CPA*, CFE
Managing Director – Advisory
KPMG LLP
345 Park Avenue
New York, NY 10154-0102
Tel: 212-872-7708
Fax: 212-409-8528
jpdooley@kpmg.com

**Licensed in PA*

Questions and Discussion

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.