The purpose of this reference guide is to provide Multi-State Information Sharing & Analysis Center (MS-ISAC) and Elections Infrastructure (EI)-ISAC members with introductory, high-level information on Deloitte’s Cyber Detect and Respond Portal (“Portal”), as well as to highlight important functions and features of the Portal and where Threat Advisories, Vulnerabilities, and other information can be obtained within the platform. This guide is also intended to aid users in navigating the Portal using screenshots along with informative boxes, arrows, text, etc. (in green font) to highlight and describe features and options for filtering searches, sorting information, configuring email notifications, etc. to improve the relevancy and usefulness of the Portal’s Cyber Threat Intelligence (CTI) and other information. However, this reference guide is not meant to be an official and exhaustive manual on all functions and features of the Portal.
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of Cyber Detect &amp; Respond Portal</td>
<td>4</td>
</tr>
<tr>
<td>MITRE ATT&amp;CK® model</td>
<td>5</td>
</tr>
<tr>
<td>Account and authentication setup in Portal</td>
<td>6</td>
</tr>
<tr>
<td>Accessing Cyber Detect and Respond Portal</td>
<td>7</td>
</tr>
<tr>
<td>Dashboard view</td>
<td>8</td>
</tr>
<tr>
<td>Threat Advisories</td>
<td></td>
</tr>
<tr>
<td>Threat Advisories view</td>
<td>16</td>
</tr>
<tr>
<td>Threat Advisory in-depth</td>
<td>18</td>
</tr>
<tr>
<td>Adding Threat Advisory Notifications</td>
<td>20</td>
</tr>
<tr>
<td>Editing Threat Advisory Notifications</td>
<td>21</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities view</td>
<td>22</td>
</tr>
<tr>
<td>Adding Vulnerability Notifications</td>
<td>24</td>
</tr>
<tr>
<td>Editing Vulnerability Notifications</td>
<td>25</td>
</tr>
<tr>
<td>Account Settings view</td>
<td>26</td>
</tr>
<tr>
<td>Bi-weekly Deloitte Cyber Threat Briefings</td>
<td>28</td>
</tr>
<tr>
<td>Deloitte Portal Terms of Use &amp; Deloitte Privacy Statement</td>
<td>29</td>
</tr>
</tbody>
</table>
Overview of Cyber Detect & Respond Portal

• Deloitte’s Cyber Detect & Respond Portal ("Portal") is a secure, online platform for obtaining industry-leading Cyber Threat Intelligence (CTI) for enhancing knowledge, understanding, and the ability to identify potential cyber threats & attacks and reduce enterprise cyber risk.

• The Portal provides in-depth analysis and recommendations from Deloitte’s worldwide network of Cyber threat analysts, with threat reports mapped to known tactics, techniques, and procedures (TTPs) of cyber threat actors and malware campaigns.
  - Threat reports include mappings of observed threat actor techniques to MITRE ATT&CK® Framework tactics to help network defenders focus threat identification and hunting on behaviors and artifacts which may indicate a cyberattack.
  - Reports include real-world samples of observed attack procedures (e.g., phishing email excerpts, sanitized malicious code).

• The Portal also enables a “pull” vs. “push” approach for obtaining CTI that is tailored to an organization’s specific IT environment and cyber threat landscape.
  - Filter by categories and keywords specific to threat actor group, malware campaign, system / application, industry, etc. to “reduce noise” and focus on cyber threat and vulnerability information most relevant to your organization.
  - Configure email-based threat notifications and reporting, vulnerability notifications, etc. according to desired frequency (e.g., daily, weekly) and filtered according to relevant categories of information, as noted above.
  - The Portal Dashboard includes numerous options for tailoring graphical information on cyber threats and vulnerabilities presented in individual “modules” (i.e., tiles) and even the ability to establish multiple dashboards, each with its own set of modules with differently configured graphical information providing a uniquely valuable view to a particular user.
Cyber Threat reports available in the Deloitte Portal include all observed techniques mapped to relevant MITRE ATT&CK® tactics, as demonstrated in the *notional* example below.

MITRE ATT&CK® includes a fully comprehensive matrix and knowledge base of adversary tactics and techniques based on real-world observations, which, along with additional information on MITRE ATT&CK®, is available at: [https://attack.mitre.org/](https://attack.mitre.org/).
Account and authentication setup in Portal

Once a new user is provisioned an account in Deloitte’s Cyber Detect and Respond Portal (“Portal”), the user will receive an invitation email, per below:

- Invitation email will be sent from: noreply@okta.com. (Please note this is a “noreply” email address which is only used to send emails but cannot receive them.)
- If you do not receive this email, please check your junk folder. If you still cannot find it, please reach out to: AthenaContactUs@deloitte.com for assistance.
- Each user must activate his/her new Okta account (per email screenshot at below left) within 30 days of email receipt or the invitation will expire.
- Another email with the Portal URL and detailed instructions for setting up account authentication will be received from: USAdvisoryCSApp001@deloitte.com.

Okta Activation - Steps following clicking the “One-Time Activation” link:
1. Type in a new password following the password requirements.
2. Select and answer a security question. This is what you will use for the password self-reset feature.
3. Choose a picture for your security image, and then click on “Create My Account.”
4. Click “Got it!” on the Okta Notification.
5. Click on the “Cyber Detect and Respond Portal” application:
6. Choose between setting up the MFA using:
   a. Okta Verify (native phone app)
   b. SMS Authentication

Okta Verify - Setup
1. Click on your device type (e.g., iOS, Android) and then click on “Next.”
2. Scan the QR barcode to add your account.
3. Click on “Send Push” to send a push notification to your phone. Tap approve on your phone and the system will log you in.

Okta SMS Authentication - Setup
1. Input your mobile phone number and click on “Send Code.”
2. Input the code you received via text message and click on Verify. The system will then log you in.
Accessing Cyber Detect & Respond Portal

Begin log-in process by entering email address and then clicking on “SIGN IN”

Cyber Detect and Respond (“Athena”) Portal URL
(Recommend bookmarking this URL in browser)

User Support Email Address: AthenaContactUs@deloitte.com

User Support Phone number: 1-833-597-5441
Dashboard view

Welcome to Cyber Detect and Respond Portal

Recent Vulnerabilities: 3
Recent Threat Advisories: 2

Threat Advisories by Threat Type

Vulnerabilities by Access Vector

Threat Advisories By TLPs

campaign threat-actor vulnerability malware

ADJACENT NETWORK LOCAL NETWORK

Count

AMBER GREEN

15 48
As shown above, there are two ways to access telephone and email contact information for “Portal Support” directly from the Portal Dashboard (i.e., landing page).
Dashboard view (cont’d)

Expands side menu options

Quick links to 3 most recent reported Vulnerabilities and 3 most recent Threat Advisories

Portal-wide search feature available throughout Portal

Cyber threat and vulnerability information graphically displayed in each module can also be displayed for a variety of time periods.

Dashboard “modules” are fully customizable and provide user-specific, graphical views of various, relevant, and continually updated sources of cyber threat and vulnerability information and intelligence.
Dashboard view (cont’d)

- Expanded direct link, side menu options
- Date range set here will apply to all data across all Threat Advisories and Vulnerabilities modules in Dashboard.
- Click on side menu links to:
  - View Threat Advisories
  - View Vulnerabilities
  - Contact Support
  - Logout
  - Return to main Dashboard view

- Feature for editing name of current dashboard
- Feature for deleting current dashboard

- Edit a Board
  - Board Name: Dashboard
  - Options: Cancel, Save

- Do you really want to delete Dashboard?
  - Options: OK, Cancel

- Date Range: [Set Date Range]
Dashboard view (cont’d)

- Create new dashboard
- Copy current dashboard
- Add module(s) to dashboard
Edit information reported by each module through configuring a wide array of data points.

Select respective report / notification milestone for setting date-based reporting in module.

Select between Threat Advisories or Vulnerabilities to display for each module.

Select date or date range for reports / notifications to display in module.
Dashboard view (cont’d)

- Filter advisories by (world) regions(s)
- Filter advisories by industry(ies) / sector(s)
- Filter advisories reported by Traffic Light Protocol (TLP) designation

Edit information reported by each module through configuring a wide array of data points
Dashboard view (cont’d)

- Filter by Advisory type:
  - Threat Notification
  - Threat Report
  - Threat Study

- Filter by Threat type:
  - Malware
  - Vulnerability
  - Campaign
  - Threat Actor

Note: This page and the 2 preceding pages provide several examples of configuration options for Threat Advisory modules. While not specifically exhibited in this reference guide, there are similar configuration options for Vulnerabilities modules. Such options for Vulnerabilities modules include filtering on access vector (local, adjacent network, or network) and access complexity (high, medium, or low).
Threat Advisories view

Threat Advisories can be accessed from any page in the Portal from the side menu.

Multiple filtering options are available, including by:
- Traffic Light Protocol (TLP)
- Industry
- Region
- Threat Type
- Advisory Type
- Date Range
Threat Advisories view (cont’d)

- Button for downloading a Threat Advisory
- Threat Advisory (email) Notifications can be set by clicking this button.
- Search bar enables focused searches for Threat Advisories containing specific keywords.
- Button for viewing details of a Threat Advisory
- Click the ‘i’ icon for a ‘Search Tips’ popup window, which is shown to the left

Sort Threat Advisories by date published in ascending or descending order.
Threat Advisory in-depth

A Threat Advisory can be downloaded as a .pdf report contained within a .zip file by clicking on this button.

These sections are included in Threat Reports only.

The structure and content of the “Threat Analysis” section of a Threat Report depends upon the “Threat Type” of the report:

- Malware
- Vulnerability
- Campaign
- Threat Actor
- Incident
Threat Advisory in-depth (cont’d)

Applicable MITRE ATT&CK Tactics, Techniques, and Descriptions of Techniques are also included in all Threat Reports.

Click this button to draft a Threat Advisory-specific email to submit relevant questions to the following, CTI analyst-monitored address: detectandrespondportal@deloitte.com.
Adding Threat Advisory Notifications

“Frequency” options include:
▪ As Soon as Possible
▪ Daily
▪ Weekly

A “Notify Time” option is required when “Daily” or “Weekly” is selected, and a “Notify Day” is also required when “Weekly” is selected.

Enter specific text (e.g., “ransomware,” “phishing,” “microsoft”) for “Query” to filter Threat Advisory Notifications.

“Advisory Types” options include:
▪ All Advisory Types
▪ Threat Notification
▪ Threat Report
▪ Threat Study

Click this button to add a Threat Advisory Notification.
Editing Threat Advisory Notifications

Click this button to edit a Threat Advisory Notification.

Modify “Frequency,” “Notify Day,” “Notify Time,” “Advisory Types,” and/or “Query” text when editing Threat Advisory Notifications

Click this button to delete a Threat Advisory Notification.
Vulnerabilities view

Vulnerabilities can be accessed from any page in the Portal from the side menu.

Multiple Vulnerabilities filtering options are available, including by:

- Access Vector
  - Network
  - Adjacent Network
  - Local

- Access Complexity
  - High
  - Medium
  - Low
Sort Vulnerabilities by Common Vulnerabilities and Exposures (CVE) identification number (https://cve.mitre.org/), Common Vulnerability Scoring System (CVSS) Base score (https://www.first.org/cvss/), or by date published in ascending or descending order.

Button for viewing details of a Vulnerability
Adding Vulnerability Notifications

The “Name” entered will appear at the top of Vulnerability Notification emails for rapid identification of associated vulnerabilities.

Enter specific text (e.g., “google,” “microsoft,” “remote execution”) for “Query” to filter Vulnerability Notifications.

A number entered here will filter Vulnerability Notifications according to a minimum Common Vulnerability Scoring System (CVSS) Base score (https://www.first.org/cvss/).
Editing Vulnerability Notifications

Click this button to edit a Vulnerability Notification.

Modify “Name,” minimum CVSS Base score, and/or “Query” text when editing Vulnerability Notifications.

Click this button to delete a Vulnerability Notification.
Account Settings view

The “Profile Information” options depicted here are available by clicking on the user’s “Settings” link at the top of any Portal page.

A user’s “Profile Information”, which can be edited as needed.
A user can edit any of his/her “Profile Information” displayed above.
Bi-weekly Deloitte Cyber Threat Briefings

- All Portal users are also invited to attend Bi-weekly Deloitte Cyber Threat Briefings. These 1-hour webcasts provide timely and relevant information on current and high-risk cyber threats, such as attack campaigns, hacker group tactics & techniques, new ransomware strains, etc.

- Each calendar invite received is specific to a particular bi-weekly webcast and Portal user and is generally sent 2 days prior to the event. You will need to click on the “Click Here to Join” link (noted in the graphic at below left). You may click on this URL directly in the email invite prior to accepting it, or any time thereafter within the calendar hold itself upon accepting the meeting invite and prior to the webcast.

- After clicking on the “Click Here to Join” link, you will be directed to the bi-weekly webcast registration webpage. In order to attend each webcast, you must first register for the event by completing the information on the left-hand side of the webpage and then clicking on the “Submit” button, as shown in the graphic at below right (see number “1”).

- Only after you first register for the webcast, will you be able to later join the event by entering your email address, which must be the same email address associated with your Portal account and the same email address used for webcast registration, in the field on the right-hand side of the same webpage and then clicking the “Log In” button (see number “2”).
Terms of Use

These Terms of Use apply to your use of the website that links to this Terms of Use document (the "Website"). To the extent there is an executed agreement with Deloitte & Touche LLP ("we" or "us") governing your licensed use of any technology, or your access to any membership or subscription offering, available on this Website (an "Agreement"), your use and access to any such technology or offering will be further governed by such Agreement. To the extent there is a conflict between these Terms of Use and an Agreement, the terms of the Agreement shall control. By using this Website, you are agreeing to these Terms of Use. If you do not agree to these Terms of Use, then you are not allowed to use this Website and should immediately terminate such usage.

Use of Content; Restrictions

Unless otherwise indicated in the relevant content, and on the condition that you comply with all of your obligations under these Terms of Use, (i) you are authorized only to view and print the content on this Website for informational, noncommercial purposes and provided that any copy of the content that you make must include the copyright notice or other attribution associated with the content; and (ii) you are not authorized to copy or use any software, proprietary processes or technology embodied or described in this Website.

You will comply with all applicable laws in accessing and using this Website. You acknowledge that we may use your personal information and data according to our Privacy Statement, set forth in the Privacy link on this Website. This Website and its contents are protected by copyright, trademark, and other laws of the United States and/or other countries. We and our licensors reserve all rights not expressly granted in these Terms of Use. References to other parties’ trademarks on this Website are for identification purposes only and do not indicate that such parties have approved this Website or any of its contents, nor should they be construed as an endorsement of them or their content by us. You will need a username and password (a "User Account") to access the Website. You are responsible for anything that happens through your User Account, unless and until you request deactivation in accordance with this Agreement. Without limiting the foregoing, you agree to the following:

• At any given time, you will create and maintain only one User Account for yourself. You cannot have multiple User Accounts for your use of the Website. Your User Account will be for you alone, and you cannot share or transfer it to anyone else.
• You shall keep your User Account, password secure and confidential.
• You shall not remove any copyright, trademark, or other proprietary rights notices found on the Website or any of its content ("Content"), including any Content from us, another Deloitte Network entity, or a third party.
• You shall not engage in any action that directly or indirectly interferes with the proper working of, or places an unreasonable load on, our or service provider's infrastructure, including spamming or the distribution of computer viruses or other malicious code.
• You shall promptly notify us upon becoming aware of any unauthorized use of your User Account or any other breach of this Agreement.

Disclaimers and Limitations of Liability

THIS WEBSITE CONTAINS GENERAL INFORMATION ONLY, AND WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THESE TERMS OF USE APPLY TO YOUR USE OF THE WEBSITE THAT LINKS TO THIS TERMS OF USE DOCUMENT (THE "WEBSITE"). TO THE EXTENT THERE IS AN EXECUTED AGREEMENT WITH DELLOITTE & TOUCHE LLP ("WE" OR "US") GOVERNING YOUR LICENSED USE OF ANY TECHNOLOGY, OR YOUR ACCESS TO ANY MEMBERSHIP OR SUBSCRIPTION OFFERING, AVAILABLE ON THIS WEBSITE (AN "AGREEMENT"), YOUR USE AND ACCESS TO ANY SUCH TECHNOLOGY OR OFFERING WILL BE FURTHER GOVERNED BY SUCH AGREEMENT. TO THE EXTENT THERE IS A CONFLICT BETWEEN THESE TERMS OF USE AND AN AGREEMENT, THE TERMS OF THE AGREEMENT SHALL CONTROL. BY USING THIS WEBSITE, YOU ARE AGREEING TO THESE TERMS OF USE. IF YOU DO NOT AGREE TO THESE TERMS OF USE, THEN YOU ARE NOT ALLOWED TO USE THIS WEBSITE AND SHOULD IMMEDIATELY TERMINATE SUCH USAGE.

Use of Content; Restrictions

Unless otherwise indicated in the relevant content, and on the condition that you comply with all of your obligations under these Terms of Use, (i) you are authorized only to view and print the content on this Website for informational, noncommercial purposes and provided that any copy of the content that you make must include the copyright notice or other attribution associated with the content; and (ii) you are not authorized to copy or use any software, proprietary processes or technology embodied or described in this Website.

You will comply with all applicable laws in accessing and using this Website. You acknowledge that we may use your personal information and data according to our Privacy Statement, set forth in the Privacy link on this Website. This Website and its contents are protected by copyright, trademark, and other laws of the United States and/or other countries. We and our licensors reserve all rights not expressly granted in these Terms of Use. References to other parties’ trademarks on this Website are for identification purposes only and do not indicate that such parties have approved this Website or any of its contents, nor should they be construed as an endorsement of them or their content by us. You will need a username and password (a "User Account") to access the Website. You are responsible for anything that happens through your User Account, unless and until you request deactivation in accordance with this Agreement. Without limiting the foregoing, you agree to the following:

• At any given time, you will create and maintain only one User Account for yourself. You cannot have multiple User Accounts for your use of the Website. Your User Account will be for you alone, and you cannot share or transfer it to anyone else.
• You shall keep your User Account, password secure and confidential.
• You shall not remove any copyright, trademark, or other proprietary rights notices found on the Website or any of its content ("Content"), including any Content from us, another Deloitte Network entity, or a third party.
• You shall not engage in any action that directly or indirectly interferes with the proper working of, or places an unreasonable load on, our or service provider's infrastructure, including spamming or the distribution of computer viruses or other malicious code.
• You shall promptly notify us upon becoming aware of any unauthorized use of your User Account or any other breach of this Agreement.

Disclaimers and Limitations of Liability

THIS WEBSITE CONTAINS GENERAL INFORMATION ONLY, AND WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

We may revise these Terms of Use at any time in our sole discretion by posting such revised Terms of Use at the Terms of Use webpage. Such revisions shall be effective as to you upon posting, unless explicitly stated by us.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, TORT, OR OTHERWISE. YOU ACKNOWLEDGE THAT WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.