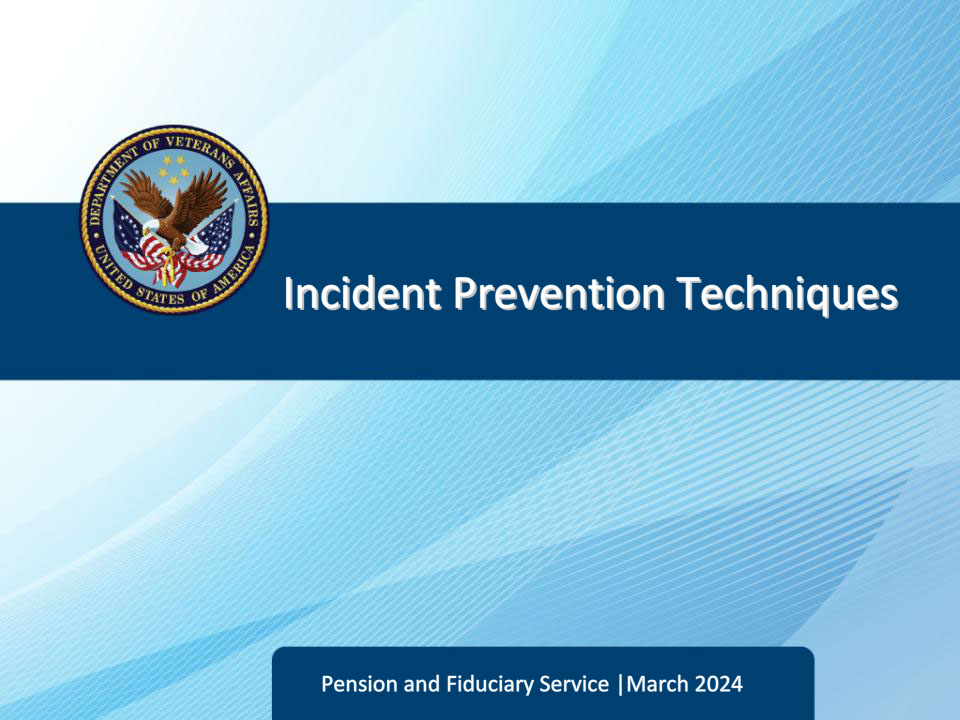
**Slide 1 - Incident Prevention Techniques**

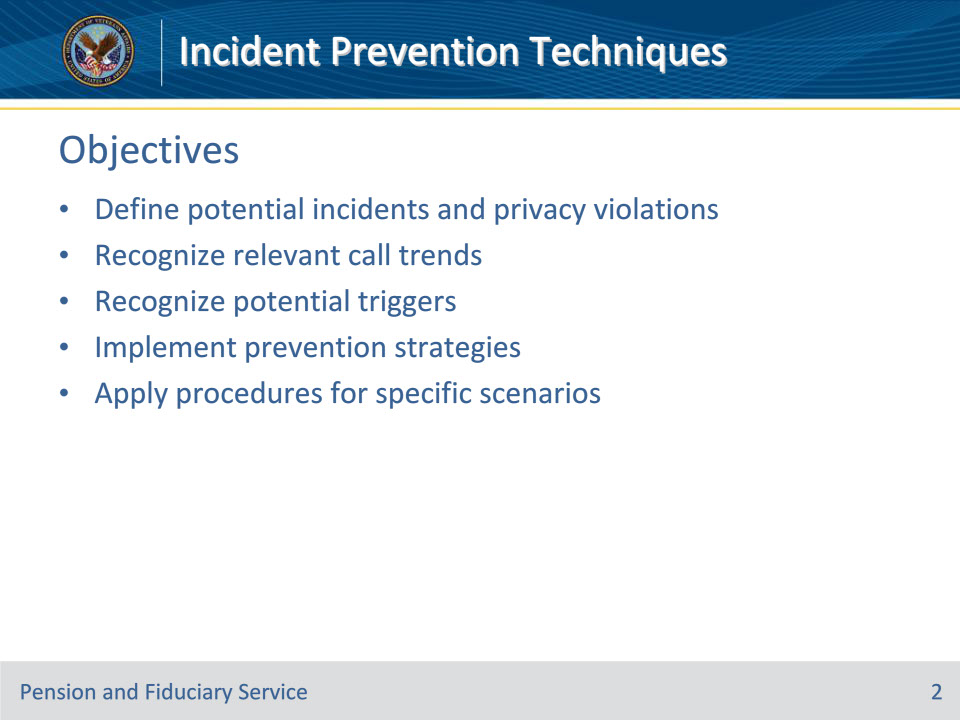


**Slide notes**

Course Description:

Welcome to the Incident Prevention Techniques training for the Fiduciary Contact Center. In this course, Legal Administration Specialists (LAS) will learn how to identify and handle potential incidents and privacy violations. They will define incidents and privacy violations, recognize trends and triggers, become familiar with prevention strategies, and recall and apply specific procedures.

**Slide 2 - Objectives**



**Slide notes**

Instructor Notes:

At the end of this lesson, given the training and references, the learner will be able to do the following:

• Define potential incidents and privacy violations

• Recognize relevant call trends

• Recognize potential triggers

• Implement prevention strategies

• Apply procedures for specific scenarios

**Slide 3 - References**



**Slide notes**

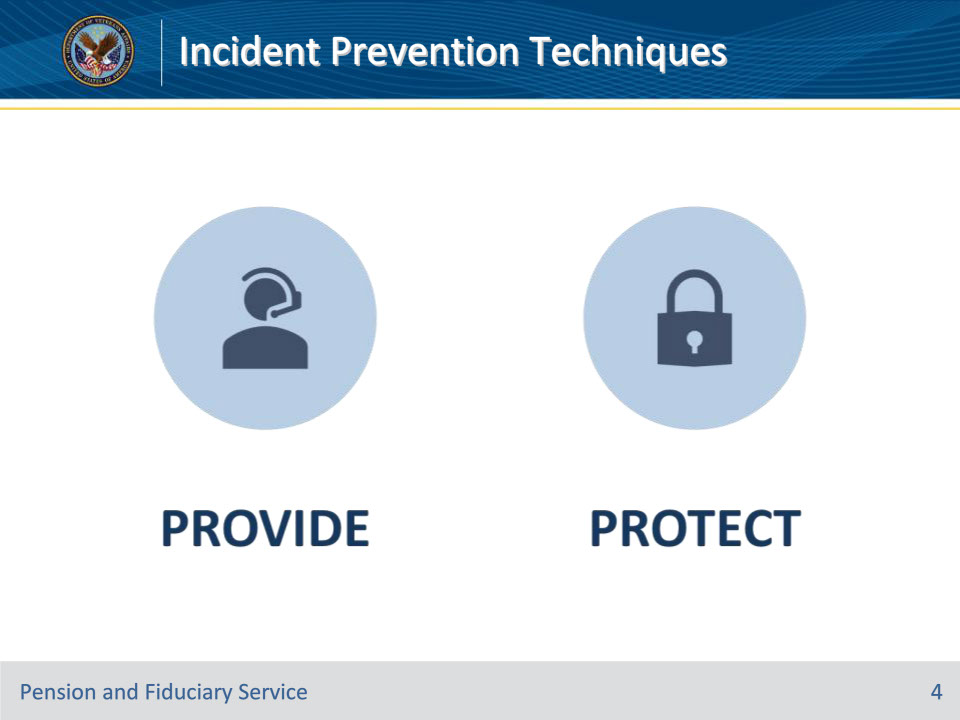
Instructor Notes:

These are the relevant references pertaining to this course:

• ID Protocol Requirements

• Identity Theft and Fraud

**Slide 4 - Slide 4**



**Slide notes**

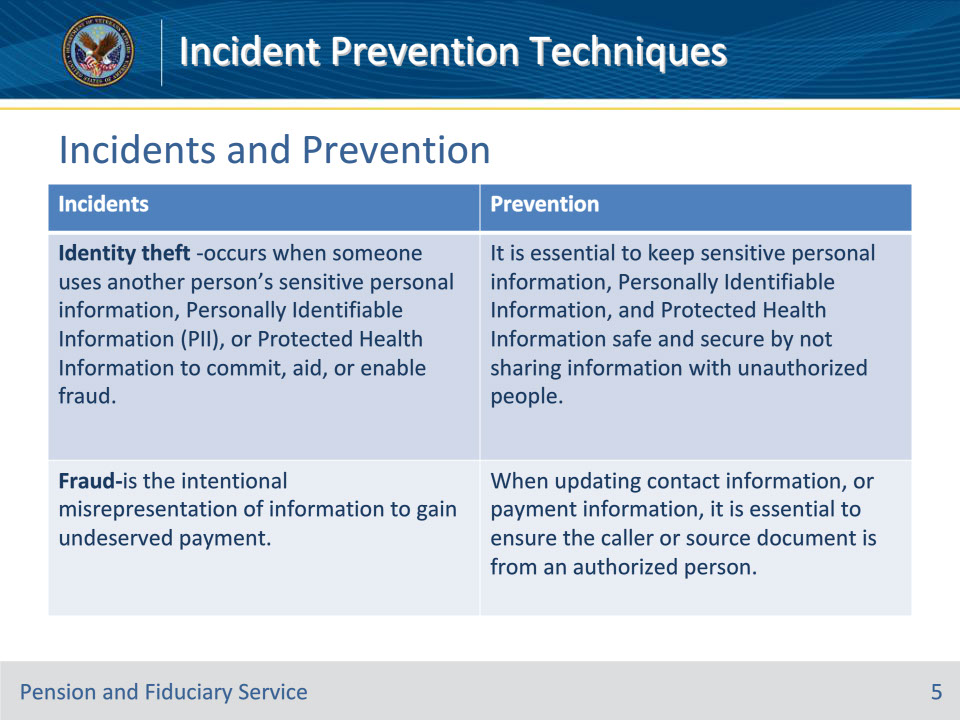
Policy Reference(s):

Instructor Notes

As an LAS, it’s crucial to understand that the Fiduciary Call Center has a dual responsibility. Not only do you provide information, but you’re also responsible for protecting sensitive information. You are the first line of defense for VA privacy, and it‘s up to you to recognize potential incidents and privacy violations. It’s a serious responsibility, but one that you should take pride in. By being vigilant and careful, you can help ensure that the beneficiaries’ information remains safe and secure.

This lesson will cover potential incidents and privacy violations. LASs must be able to identify and take the appropriate action on potential incidents and privacy violations. This training is designed to develop the LASs skills and techniques for recognizing and reacting to potential incidents. These skills and techniques give LASs the confidence they need to assess a situation and decide if they can move forward with updating contact information or taking appropriate actions necessary to address potential incidents and privacy violations.

**Slide 5 - Incidents and Prevention**



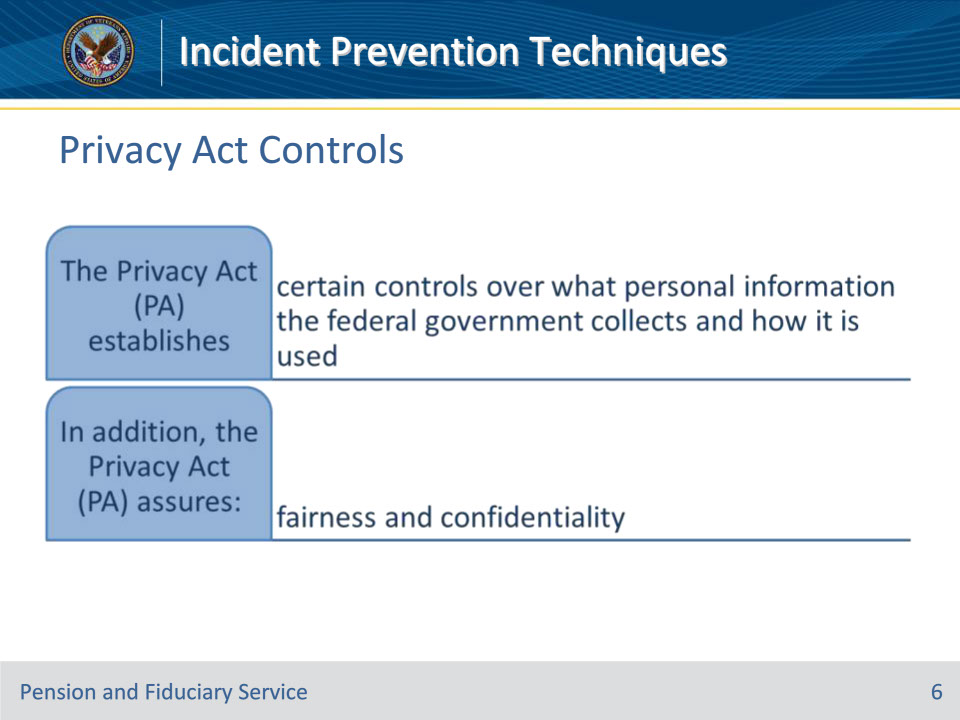
**Slide notes**

Policy Reference(s):

Instructor Notes

It’s crucial to keep in mind that Veterans/beneficiaries are frequently targeted by identity thieves. These criminals use sensitive personal information, including Personally Identifiable Information (PII) and Protected Health Information, to carry out fraudulent activities. It’s disheartening that those who have bravely served our country are at risk of falling victim to this type of crime. Therefore, it’s imperative to take measures to safeguard against such occurrences. Whenever you update contact or payment information, make sure that the caller or source document is coming from an authorized person. In this presentation, we will delve deeper into this topic and discuss ways to prevent privacy violations.

**Slide 6 - Privacy Act Controls**



**Slide notes**

Policy Reference(s):

Instructor Notes

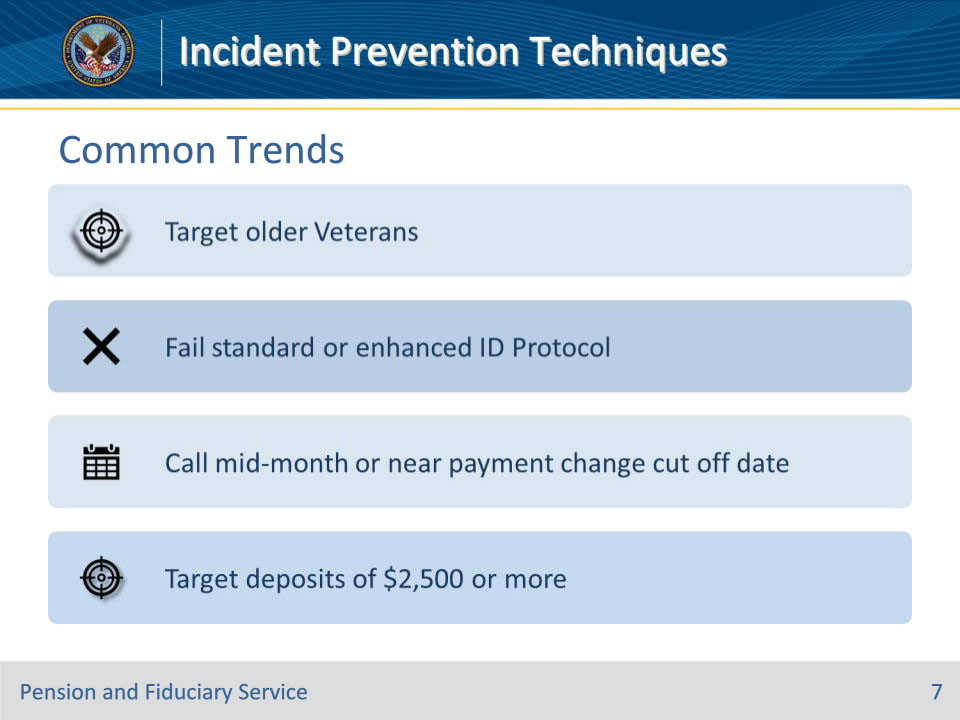
The Privacy Act (PA) establishes certain controls over what personal information the federal government collects and how it is used. In addition, the Privacy Act (PA) assures:

• Fairness to an individual by requiring that records be maintained with reasonable accuracy and that safeguards against invasion of an individual’s personal privacy are maintained, and

• Confidentiality of any VA record about a person is maintained with reasonable accuracy and that the record is safeguarded against the invasion of personal privacy.

Once situations arise that violate the two assurances, as LASs, you play an essential role reporting the potential incident/privacy violation(s). For VA purposes, potential incident(s) represent situations that can cause harm, is causing harm, or continues to cause undue harm to the Veteran/beneficiary. Further, that incident can have a negative impact on the service or quality of service(s) offered by the VA to the Veteran/beneficiary

**Slide 7 - Common Trends**



**Slide notes**

Policy Reference(s):

Instructor Notes

Potential incident/privacy violation common trends include:

• The tendency to target older Veterans/beneficiaries: Financial scams targeting seniors have grown over the years, but often are underreported. These scams can cause severe financial and other devastating results.

• Most likely to occur mid-month on or near the payment change cutoff date: Imposters do this to ensure the next payment is routed to them.

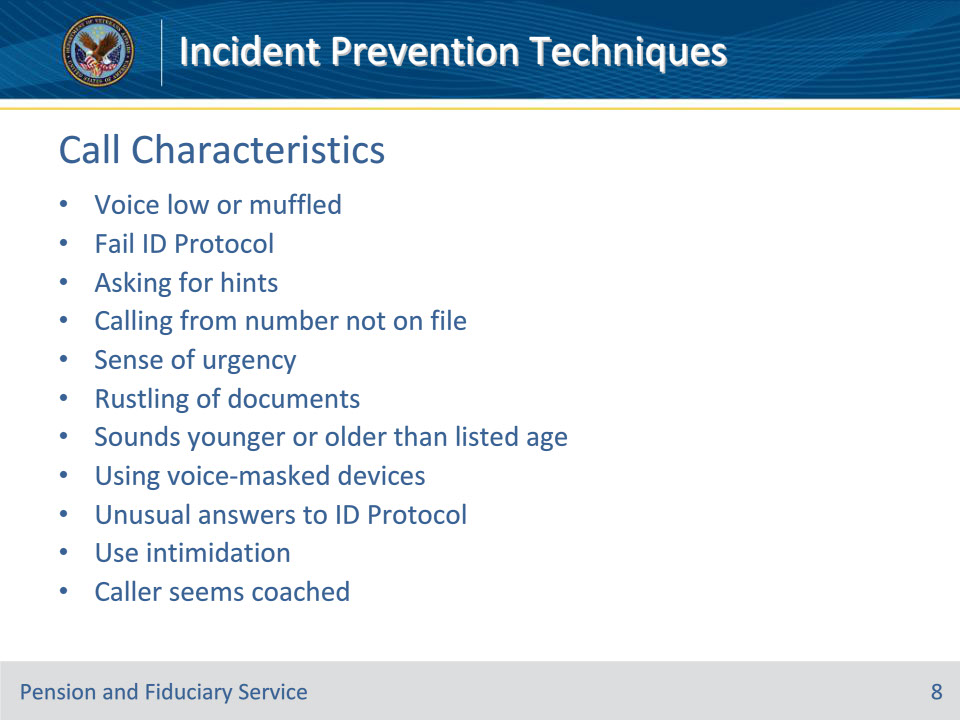
• The inclination to target Veterans/beneficiaries with recurring monthly deposits of $2,500.00 or greater: It’s important to remember that imposters can target anyone, regardless of the payment amount. While it’s true that they may go for bigger amounts, it’s also possible for them to exploit vulnerabilities in smaller payments.

• Imposters tend to fail standard and enhanced ID protocol: Fail requirements at first attempt; make multiple attempts at providing the information.

• Uncertainty of PII, current direct deposit, and/or contact information

• Verbalization of SSN in an unorthodox pattern (should be in the pattern of xxx-xx-xxxx)

**Slide 8 - Call Characteristics**



**Slide notes**

Policy Reference(s):

Instructor Notes

Call characteristics that LASs should be listening for are:

• The caller’s voice low in volume and/or muffled

• LASs frequently asking the caller to “speak up” or repeat information

• The failure of standard and/or enhanced ID Protocol requirements at first attempt

• The caller’s trying to convince the LAS to provide hints/information or additional opportunities to complete standard and/or enhanced ID Protocol.

• The caller is calling from a number that is not associated with the Veteran/beneficiary’s record

• Requestor exhibits a sense of urgency and attempts to play on emotions.

• Requestor using VA correspondence or other documents to answer basic identification questions.

• Caller rustling/scrambling documents to provide answers to ID Protocol questions.

• Caller sounds younger/older than the DOB in the system of record.

• Calling near the payment change cutoff date

• Asking the payment change cutoff date

• Caller using voice-masked talking devices

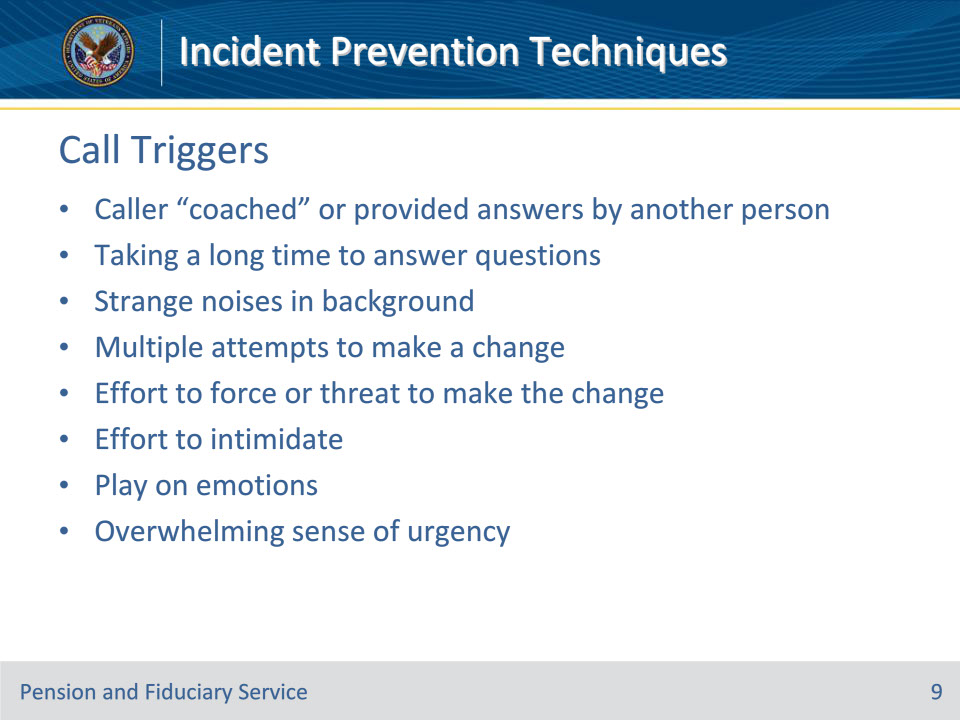
• Caller using unusual language when ID Protocol questions are asked

• Imposters attempt to intimidate or force LAS to complete the change of contact information.

• Requestor is “coached” or provided answers by another person

LASs must be aware of and consider the potential for unauthorized changes when attempting to identify potential incidents on every contact information update request. They must focus on administering the mandatory ID Protocol requirements as an essential incident prevention technique.

**Slide 9 - Call Triggers**



**Slide notes**

Policy Reference(s):

Instructor Notes

There are call triggers that should get LASs attention to recognize there is an “at risk” event potentially occurring during the telephone interaction.

While addressing a caller, consider the following to determine if there is a potential incident/privacy violation:

• Is the caller being “coached” or provided answers by another person?

• Is the caller taking a long time to answer the questions?

• Are there any strange noise(s) in the background?

• Are there multiple attempts to make a change?

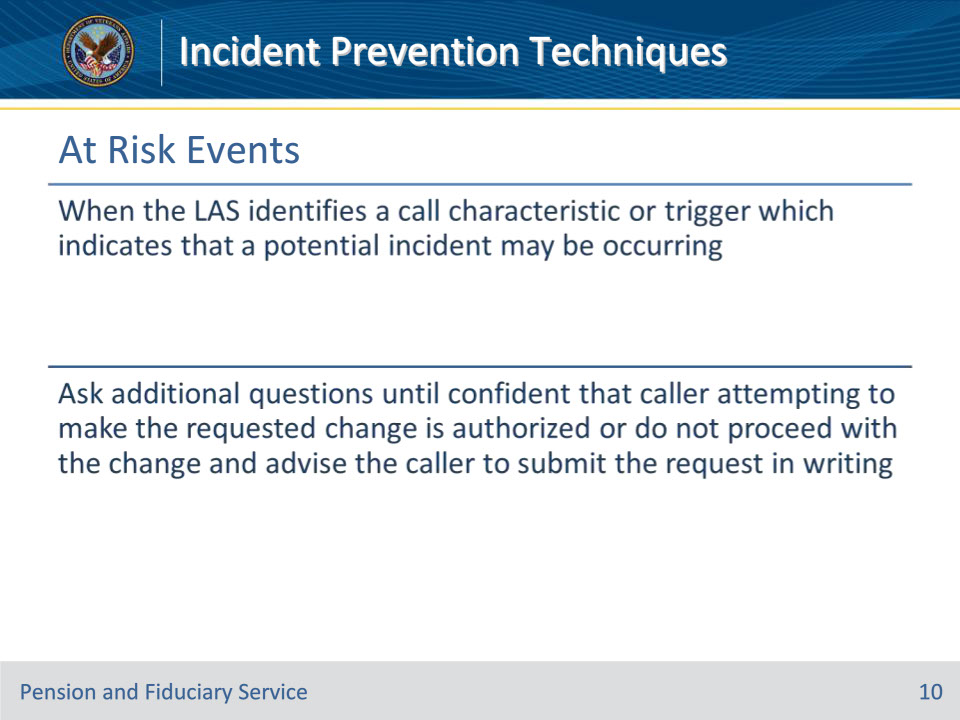
• Is there an effort to force or threat to make the change?

• Is there an effort to intimidate the LAS?

• Is there a play on emotions? (e.g., compliments to sway actions)

• Is there an overwhelming sense of urgency?

**Slide 10 - At Risk Events**



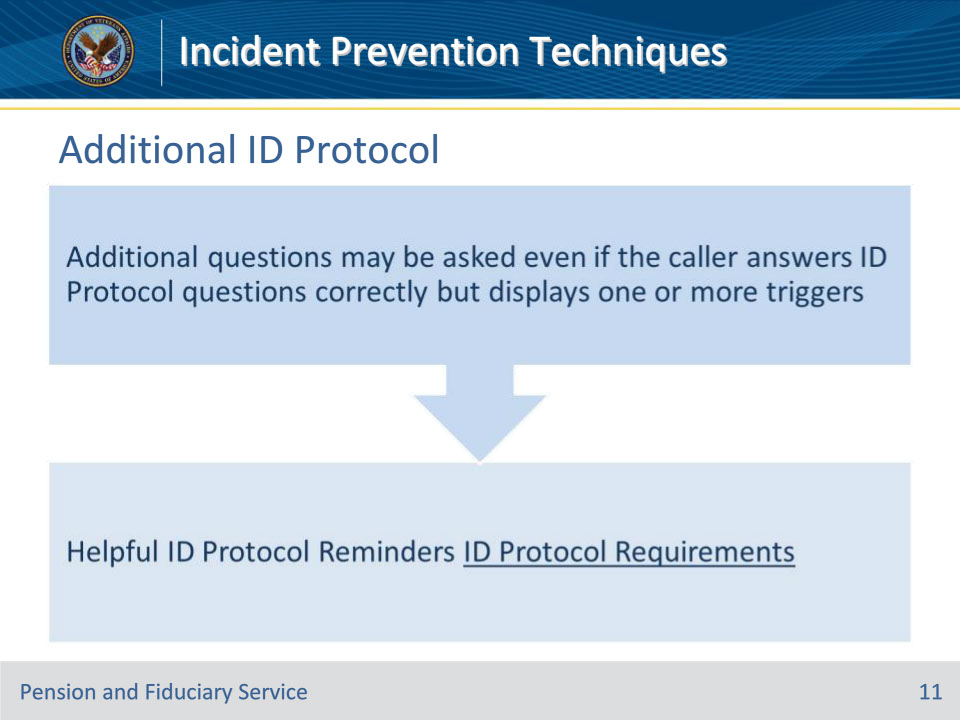
**Slide notes**

Policy Reference(s):

Instructor Notes

An “at risk” event is when the LAS identifies one of the previously mentioned call characteristics or incidents are occurring. The LAS should listen for call triggers on each phone call where the caller attempts to change contact or direct deposit information. When the LAS has identified an “at risk” event potentially occurring, additional questions should be asked until the LAS feels confident that the person attempting to make the requested change is authorized. If the LAS does not feel comfortable with making the change because of at-risk factors, they can ask additional questions until they are comfortable or choose not to proceed with the change and advise the caller to submit the request in writing. Ensure this information is documented on a VA Form 27-0820.

**Slide 11 - Additional ID Protocol**



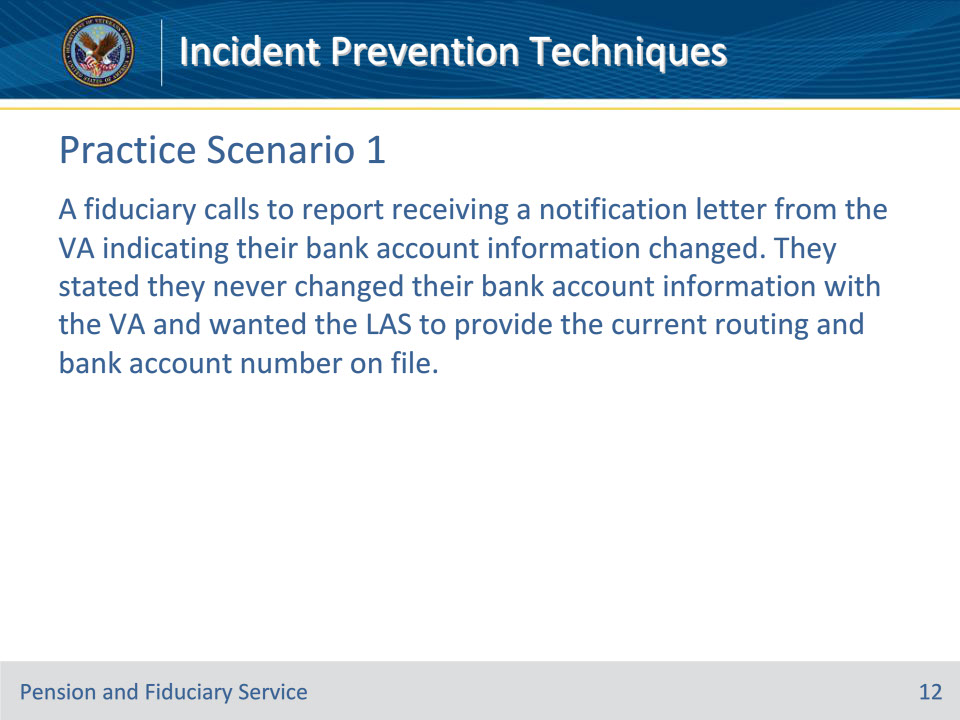
**Slide notes**

Policy Reference(s):

Instructor Notes

Instructor Demonstration: Review the link on the slide for ID Protocol Requirements and point out the “ID Protocol Reminders”

**Slide 12 - Practice Scenario 1**



**Slide notes**

Policy Reference(s):

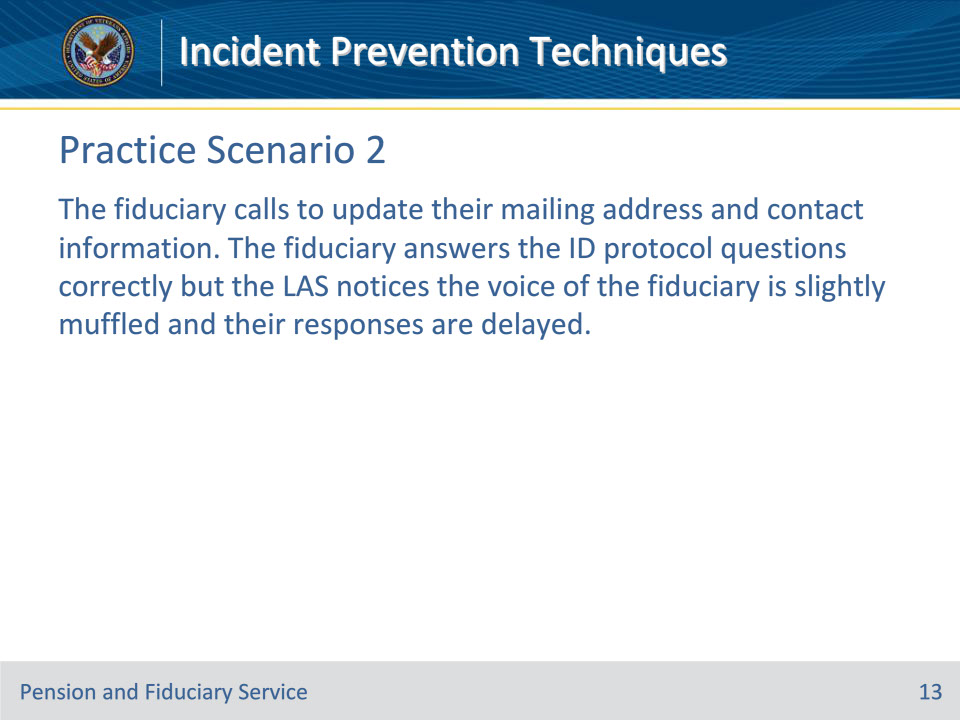
Instructor Notes

Scenario: A fiduciary calls to report receiving a notification letter from the VA indicating their bank account information changed. They stated they never changed their bank account information with the VA and wanted the LAS to provide the current routing and bank account number on file.

Question: What action and/or steps should you take as the LAS?

Answer: In this scenario, the LAS must first identify the caller by asking ID protocol questions. They should encourage the caller to provide the account information instead of giving the fiduciary the account details.

**Slide 13 - Practice Scenario 2**



**Slide notes**

Policy Reference(s):

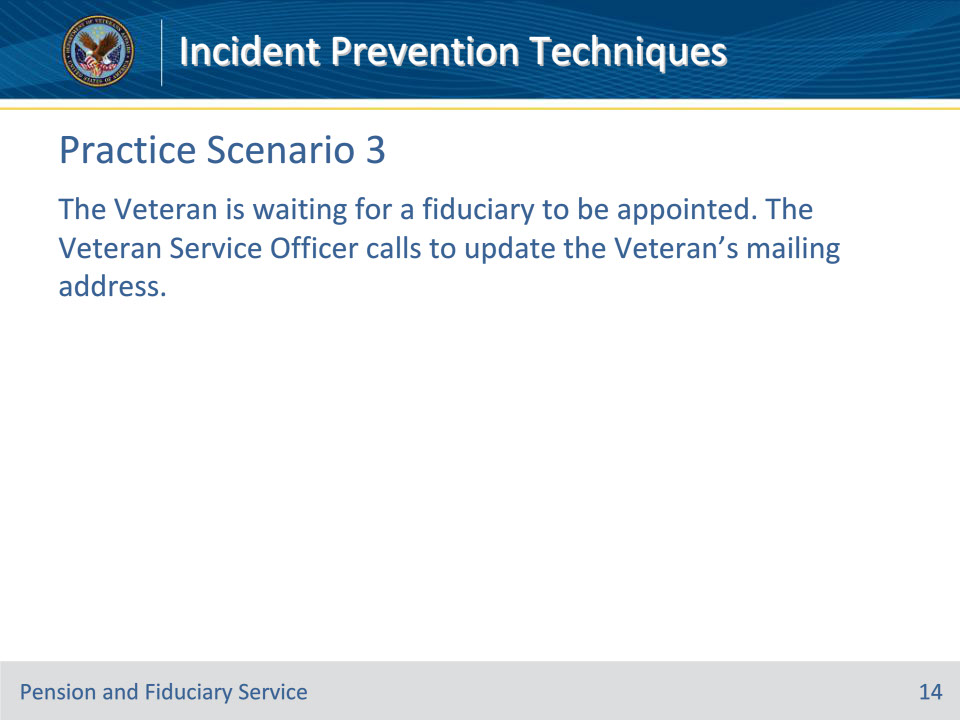
Instructor Notes

Scenario: The fiduciary calls to update their mailing address and contact information. The fiduciary answers the ID protocol questions correctly but the LAS notices the voice of the fiduciary is slightly muffled and their responses are delayed.

Question: What action and/or steps should you take as the LAS?

Answer: In this scenario, the LAS must understand that this may be an “at-risk event.” They should recognize the need to ask additional questions. Additional questions may be asked even if the caller answers ID Protocol questions correctly but displays one or more of the before-mentioned call characteristics or call triggers.

**Slide 14 - Practice Scenario 3**



**Slide notes**

Policy Reference(s):

Instructor Notes

Scenario: The Veteran is waiting for a fiduciary to be appointed. The Veteran Service Officer calls to update the Veteran’s mailing address.

Question: What action and/or steps should you take as the LAS?

Answer: In this scenario, the LAS must recognize that the VSO is considered a First-party caller.

**Slide 15 - Questions?**



**Slide notes**

Instructor Notes:

(Recall) These are our learning objectives as stated from the beginning of the training:

• Define potential incidents and privacy violations

• Recognize relevant call trends

• Recognize potential triggers

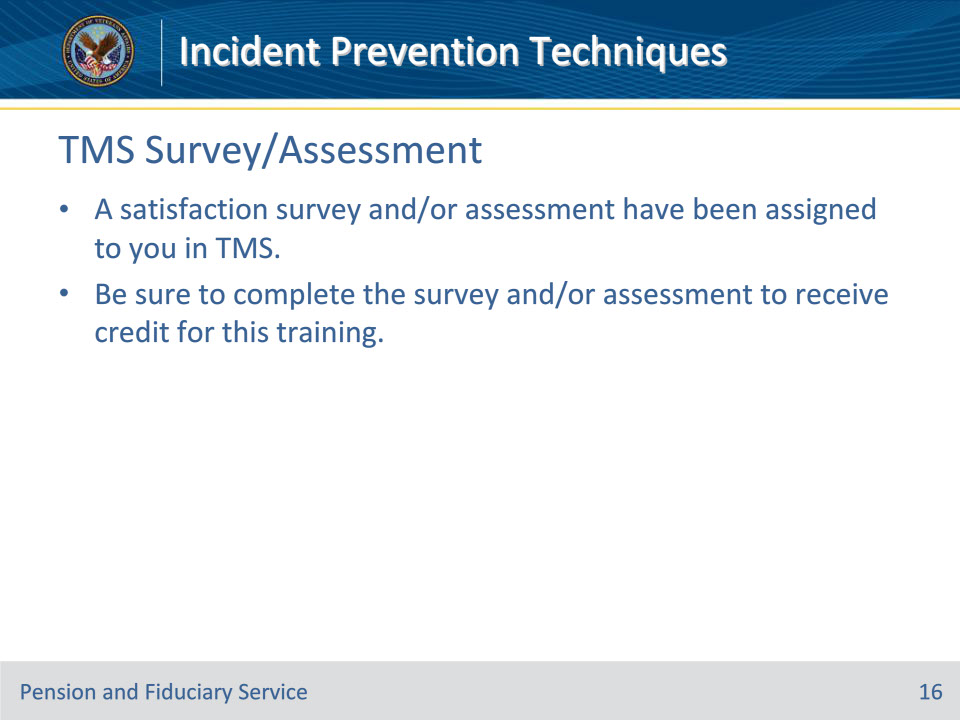
• Implement prevention strategies

• Apply procedures for specific scenarios

Are there any additional questions?

Questions should be filtered through your QRT team. They will submit your questions to the Field Inquiry Tool (FIT) on your behalf.

**Slide 16 - TMS Survey/Assessment**



**Slide notes**

Instructor Notes

A satisfaction survey and/or assessment have been assigned to you in TMS.

Be sure to complete the survey and/or assessment to receive credit for this training.