Instructional Analysis of Call Center Security Training for New Hire Investigators

TABLE OF CONTENTS

1. Project Overview

This security training is an addition to the current curriculum designed for new hire call center investigators that are both internal and external hires. The security investigator role is considered the hardest and most complex customer service role within the financial institution. The training consists of a four-week program that is complex and fast-paced. The technical training is delivered over an eight-day period and consists of basic skills, system tutorials and procedural lessons. The training is structured to teach the skills and systems used based on the call type.

Several gaps were identified with existing curriculum through analysis of learner's and feedback provided during and post training. Additional gaps were identified from feedback provided by security leadership on new investigators' performance.

This project concentrates on providing basic knowledge of fraud/scams and necessary soft skills that will be facilitated prior to procedural and technical training through a self-paced independent eLearning. This additional module will provide a high-level overview of different types of fraud scams and their relation to account reviews conducted by security investigators. It outlines how victims fall prey to fraudsters, red flags associated with potential scams, probing questions investigators should ask victims and ways to educate victims on how to prevent and protect themselves in the future. Security investigators will complete two assessments to evaluate their understanding of the material. The initial assessment will consist of eleven multiple-choice questions incorporated at the end of the eLearning. The second evaluation will be conducted utilizing gamified simulations. The investigators will be provided with six different call scenarios and will have to answer different multiple-choice questions for each. Investigators will be required to pass both assessments with an 80% or higher.

In addition to eLearning this project includes suggested role play activities to be incorporated into different clusters of the existing curriculum to address the lack of hands-on training simulations. During the pilot phase, the role play scenarios will be instructor led and will be simulated, as best as possible, using production systems. If the formal data indicates that the pilot is a success, the mock call scenario will be integrated into a gamified simulation that new hire investigators can use to practice actual call scenarios in a comprehensive hands-on environment.

2. Identify Instructional Goals

Needs Analysis:

The training department identified several gaps after conducting a front-end analysis on the security investigators curriculum. *See Appendix D for needs assessment template used. (please note the information from the actual assessment has been removed).*

The needs analysis conducted on the security training curriculum is based on feedback provided by new hires through training evaluation surveys conducted weekly during training. New hire trainees reported inadequate or lack of soft skills training for their job role. Specifically in three correlated areas: In-depth understanding of how fraud/scams work, appropriate verbiage to use, and how to educate victims on ways to protect and prevent falling victim again. New hires also reported a lack of and need for more hands-on practice such as simulation or role play scenarios. *See Appendix A for weekly evaluation surveys.*

Additional surveys were given to security leadership 30- and 60- days post training to gather feedback on investigator's performance. Leadership reported low performance rates of new hires immediately post-training. It was also reported that most new hires required additional and/or re-training due to improper training. *See Appendix B for Leadership Evaluations.*

Based on the survey results Security leadership met with the training department to conduct a specific needs analysis for objectives needed immediately to provide adequate training in soft skills.

Gaps Identified:

- Lack of soft skills training.
- Little to no understanding of fraud/scams and trends.
- Inability to educate on prevention protection.
- No hands-on practice: Roleplay or simulation.
- Outdated curriculum.

Proposed Instructional Goals:

Instructional Goal: *Intellectual Skill (ill-structured problem solving)*
New hire security trainees will identify the fraud scam type customers fell victim to secure accounts and educate members on preventative measures.

The objective of the proposed curricula is to enhance current training materials to help new investigators gain a better comprehension of fraud scams related to various real world fraud scenarios while helping victims with accounts via phone to improve skills for higher success rates after training.

The goal is to revamp the curriculum to add additional soft skills training. The training team has proposed the addition of a 30-minute eLearning training model to be added prior to technical skills training to address the immediate lack of soft and entry skills needed to perform job duties. It

is also proposing the addition of 30-minute formal role-play simulation training clusters to certain technical skills modules to provide hands-on real-world training in a controlled learning environment.

Instructional Goals for Fraud/Scam Lesson:

- Ensure the curriculum is up to date in comparison to Manuals.
- Create additional modules for soft skills training.
- Increase awareness and understanding of fraud/scams.
- Develop effective communication with appropriate verbiage.
- Develop strategies and techniques to educate fraud/scam victims on ways to protect and prevent future activity.

Instructional Goals for Fraud/Scam Lesson:

- Create an engaging curriculum that incorporates different practice simulation activities.
    - Role Play Scenarios for different call types.
    - Simulated hands-on practice of different procedural steps within systems used.

FORT Training Analysis

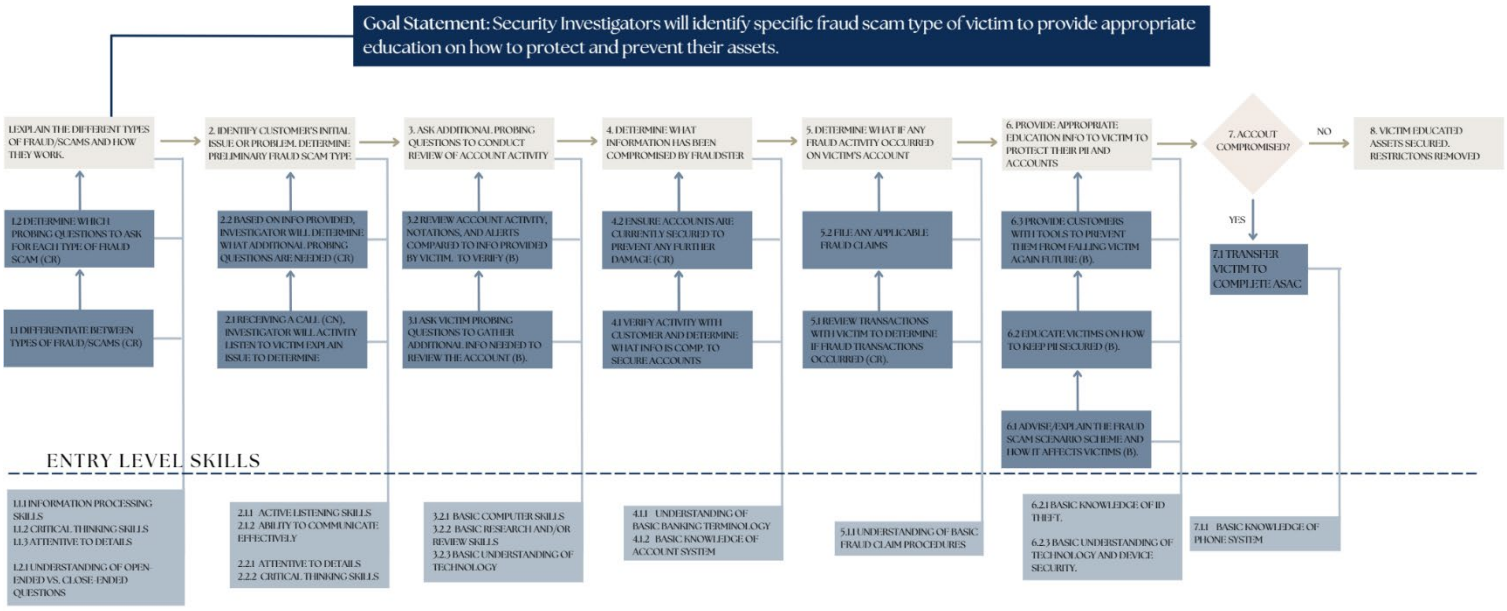
Job to be Analyzed:	Security Investigator					
Goal	Job behaviors	Skills / Knowledge		Skills / Knowledge Level	Need for training	Training recommendations
What organizational goal are we trying to achieve?	*Which job behaviors contribute to achieving this goal?*	*Which skills and knowledge components are required to display the relevant behaviors?*		*What are the levels of the required skills and knowledge*	*What is the level of need for training?*	*What type of training is needed to close the skills and knowledge gaps?*
Increase knowledge and skills performance immediately post-training	Little to no knowledge and/or understanding of fraud scams.	Knowledge	**Fraud Scam Trends** Knowledge of different types of fraud scam trends and how they work.	1	High training need	Self-paced learning module- Online Asynchronous.
		Skill	**Red Flags and Probing Questions** Know the red flags and which probing questions to ask based on fraud scam type.	1	High training need	Self-paced learning module- Online Asynchronous.
			Retention and Transfer to Job Skills Ability to measure retention and transfer of basic job knowledge prior to procedural skills training.	1	High training need	Simulated assessment for understanding and retention.
	Ability to Educate members appropriately on keeping assets secured as well as preventative measures.	Skill	**Prevention and Protection Verbiage** Effectively communicate information to scam victrims.	3	Low training need	Self-paced learning module- Online Asynchronous.
		Skill	**Retention and Transfer to Job Skills** Ability to measure retention and transfer of basic job knowledge priort to field training.	2	High training need	Gamified assessment: Mock call scenario simulations with multiple choice assessment
		Skill	**Simulated Hands on Training** Increase hands on training in systems and through real-wrold scenarios.	2	High training need	Instructor led role-play of real-world scenarios

3. Goal Analysis

Target Audience: New hire security call center trainees.

Performance Issue:
Inability to identify types of fraud scams to properly educate victims on ways to protect and prevent falling victim again in the future.

Complete Task:
Investigators will identify fraud scam types to assist victims with securing accounts as well as provide appropriate education for prevention and protection.



Goal Analysis	Subordinate Skill	Entry-Level Skills
1. Explain the different types of fraud/scams and how they work.	1.1 Differentiate between types of fraud/scams (CR). 1.2 Determine which probing questions to ask for each type of fraud/scam (CR).	1.1.1 Information processing skill. 1.1.2 Critical thinking skills. 1.1.3 Attentive to details. 1.2.1 Understanding of open-ended vs. close-ended questions.
2. Identify the customer's initial issue or problem. Determine preliminary fraud scam type.	2.1 Receiving a call (CN), investigator will actively listen to the victim explain issues or problems(B) to determine the type of fraud scam (CR). 2.2 Based on information provided, the investigator will determine what additional information is needed to ensure they have all the information needed to review the account (CR).	2.1.1 Active listening skills. 2.1.2 Ability to tactfully communicate with victims. 2.2.1 Attentive to details. 2.2.2 Critical thinking skills.

3. Ask additional probing questions to conduct review of account activity.	3.1. Ask victim probing questions to gather additional information needed to review the account (B). 3.2. Review account activity, notations, and alerts on account to compare it with the information provided by customer. 3.3 Determine the fraud scam type (B).	3.2.1 Basic computer skills. 3.2.2 Basic research and/or review skills. 3.2.3 Basic understanding of technology
4. Determine what information has been compromised by fraudster	4.1. Verify activity and determine what information has been compromised to ensure the account is secured (CR). 4.2 Ensure accounts are currently secured to prevent any further damage (CR).	4.1.1 Understanding of basic banking terminology. 4.1.2 Basic knowledge of account system.
5. Determine what if any fraud activity occurred on victim's account	5.1 Review account activity and transactions with victim to determine what if any fraud transactions occurred (CR). 5.2 File a claim (B).	5.1.1 Understanding of basic fraud claim procedures.
6. Provide appropriate educational information to victim to protect their Personal Identification Information and accounts	6.1 Advise/explain the fraud scam scenario scheme and how it affects victims (B). 6.2 Educate victims on how to keep personal identification information secure (B). 6.3 Provide customers with additional tools to prevent them from falling victim to future fraud scam attempts. (B).	6.2.1 Basic knowledge of ID theft. 6.3.1 Basic understanding of technology and device security.
7. Have victim close and open new accounts and/or change login credentials if needed	7.1 Transfer customers with compromised accounts to appropriate department to close/open new accounts and change login credentials (B).	7.1.1 Basic knowledge of phone system

4. Learner Analysis

Target Audience: New hire security call center trainees.

Learners are newly hired Security Investigators both internally and externally in the contact center of a financial institution. The educational requirement is a high school diploma or higher. Banking, fraud knowledge, or security experience is desired but not required. New hires are diverse in skills, subject knowledge, education, age, gender, goals, abilities, and other characteristics.

Information Categories	Data Sources	Learner Characteristics
1. Entry skills	Interviews/Resume, Previous trainee synopsis	Learners: New hire security investigators both internal and external. Entry Level Skills required would be: Information processing skills Critical thinking skills Active listening Skills Ability to communicate effectively Attentive to Details Understanding of open-ended vs. Close-ended questions Basic computer skills Basic research and/or review skills Basic understanding of technology and device security Basic knowledge of identity theft Basic knowledge of phone system
2. Prior knowledge of the topic	Supervisor interviews, Previous observations, Previous trainee survey results	New hires knowledge can range anywhere between no knowledge to subject matter experts.
3. Attitudes towards content	Previous class observations, Training evaluation survey	The new hire security investigator training is a four-week training. The first week is an onboarding week that consists of a high-level overview of the security department and four days of job shadowing. • Previous survey feedback received: new hires did not feel this week prepared them for their role. This time could be better utilized. The second and third week focus on curriculum, e-Learnings, and engagement activities. • Previous survey feedback received: Several gaps identified by new hires. Lack of training on different types of fraud/scams and how to educate members. Lack of hands-on training for systems used. The last week of training consists of all field exercise days. Investigators are partnered with Mentors to perform job duties. • Previous survey feedback received: new hires have reported not feeling prepared for job duties. Specifically stating, due to the amount of material covered, training was not long enough.

4. Attitudes towards potential delivery	Previous class observations, Training evaluation survey	Training is delivered in a variety of settings: traditional in-person, Virtual or a combination of both. The new hire trainees are required to be on campus in person. However, the training may still take place virtually. • Previous survey feedback received: new hires have stated that traditional in-person training is preferred due to the number of systems used and lack of hands-on training.
5. Motivation for instruction (ARCS)	Previous class observations, Training evaluation survey	This section of the course is being added to provide investigators with a basic understanding of the different types of fraud scams and how they work. This will better prepare investigators for job duties post training.
6. Educational & ability levels	Previous class observations	This role is considered an entry level position. Banking and/or fraud/security experience is desired but not required. An educational requirement is a high school diploma or higher. New hires are diverse in both education and abilities.
7. General Learning Preferences	Training evaluation survey	Previous survey feedback received: new hires have stated that traditional in-person training is preferred due to the number of systems used and lack of hands-on training.
8.Attitudes towards training organization	Training evaluation survey	Previous survey feedback received: new hires have expressed that the skills and technical training is unorganized and confusing at times.
9. General group characteristics	Previous class observations	Characteristics: age, sex, race, education, experience: banking and/or Fraud/scam knowledge, interests, ability, and culture is diverse. Class Size: Vary from 1-7 investigators per trainer per class.

5. Performance Context

Newly hired investigators are required to be on campus in person regardless of the delivery method. Performance will take place on site for the last week of training when investigators begin taking calls. Post-training investigators are expected to report to campus three days a week for their first three months.

Information Categories	Data Sources	Performance Site Characteristics
1. Managerial/supervisory support	Previous class observations	Managerial/Supervisory support during training will be from a distance. During training the facilitator is the acting leadership. They provide communication between new hires and their direct leadership until training is complete.
2. Physical aspects of site	Previous class observations	**Number:** There are two sites new hires could potentially perform job duties. On site/campus or working from home if they meet the company criterion for remote work. **Facilities:** On campus investigators will reserve a desk up to three weeks in advance. They do not have permanent desks (unless they are full-time campus employees). Therefore, the investigators desk could change daily. Post training learners are required to report to campus three days a week and have the choice to work remotely the other two days. **Resources:** Intranet manuals, OneNote participant guides and jobs aids will be provided for new hires to use during and post training. **Equipment:** New hires will be provided with all the necessary equipment to perform job duties both onsite and remote. **Timing:** This training is always Monday – Friday from 8:00 am – 4:30 pm. Lasts a total of four weeks.
3. Social aspects of site	Previous class observations	**Interaction:** Using demonstration, role play, and scenario-based learning will encourage the sales associates to work together as a team. They can pull from their experiences on the sales floor to enhance critical thinking and problem solving.
4. Relevance of skills to the workplace	Leadership feedback, Previous class observation, Training evaluation survey	Leadership has requested additional training for certain areas within the new hire training curriculum. Gaps have been identified through feedback provided by new hires on weekly evaluation surveys conducted. Additional gaps have been identified by a trainer who served as a subject matter expert previously.

6. Learning Context

Training is delivered in a variety of settings: traditional in-person, Virtual or a combination of both. There are two campus locations investigators may be reporting too. There are two sites are in different states. One location only allows for remote training while the second site can accommodate both remote and traditional in-person training.

Information Categories	Data Sources	Performance Site Characteristics
1. Number/Nature of sites	Training Department	**Number:** There are two sites new hires could potentially be at for training. One location only allows for remote training while the second site can accommodate both remote and traditional in-person training. **Facilities:** In-person training is held in a designated training room through the entirety of the class. Virtual training is conducted through a chat-based workspace with video capabilities. The learner will join the virtual class from their work desk where they will also perform their job duties. Learners are required to report to campus for the entirety of training. Post training learners are required to report to campus three days a week and have the choice to work remotely the other two days. **Resources:** Intranet manuals, OneNote participant guides and jobs aids will be provided for new hires to use during and post training. **Equipment:** New hires will be provided with all the necessary equipment to perform job duties both on site and remote. **Constraints:** If new hires are located at both sites partial class could be on site while the second site joins virtually.
2. Site compatibility with instructional needs	Training department, observation	**Instructional Strategies:** Instruction is designed primarily for a remote or virtual training environment and is a uniformed curriculum for both internal and external hires. **Delivery**: All materials are electronic and new hires must be granted access. **Time:** 4 weeks total. Including onboarding and field exercises. **Personnel**: Security Trainer, Training leadership and Security investigator leadership.
3. Site compatibility with learner needs	Training department, observation	**Location/Convenience:** New hires are required to be on site for the entirety of training regardless of if training is in-person or virtual. **Space/Equipment:** New hires will be provided with all the necessary equipment to perform job duties both virtually and in-person.

4. Feasibility for simulating workplace	Training department, observation	**Supervisory Characteristics:** Supervisors will communicate with trainees via chat-based workspace throughout training. **Characteristics:** This training primarily consists of role play scenarios and examples that can be discussed. Real time examples that can be used to demonstrate scenarios. **Social Characteristics:** Learners are paired with Mentors and SMEs for additional guidance and assistance during fields and three months post training.

7. Assessment Plan

New hire Investigators will be assessed during the interview process to see if they possess entry-level skills needed. There will be required eLearnings that investigators will take through the four-week training course and must complete all eLearning courses with a passing grade of 80% or higher. In addition to the required eLearning courses, investigators will be audited on three calls and must score an average of 80% or higher to complete their training. *See Appendix C for Call Audit Rubric.*

Test Type	**Designer's Decision**	**Objectives Typically Tested**
1. Entry skills Test	Target learners will possess the entry skills needed. They will be ready to enter instructions.	No test for entry skills. This will be assessed by leadership during interview and review of resume.
2. Pretest	Learners are both internal and external hires with and without any knowledge or background with fraud scams. Learners have previously mastered the entry level skills needed. Investigators will need to establish basic knowledge and understanding of fraud scams and how to ask customers probing questions.	Investigators will take an eLearning that should take approximately 30-40minutes that will provide an overview of Cybersecurity scams. It will provide lists of probing questions to ask customers for each scam type as well as techniques with verbiage on prevention and protection education. There will be an 11-question quiz at the end of the eLearning that learners will need to pass with an 80% or higher.
3. Practice test	To assess if learners are retaining intended knowledge and skills, they will practice mock role-play call scenarios for each scam type at the end of each cluster.	For each cluster (each scam scenario investigators might encounter with customers on the phone) investigators will practice role playing a mock call with trainer. The trainer will monitor the investigators performance and knowledge to determine if the learner is able to perform duties properly. Instructor will assess each learner and evaluate what information or procedures need to be reviewed before progressing with the next lesson.
4. Posttest	Investigators will be audited by trainer on three calls selected at random. Learners are required to pass their call audits with an average of 80% or higher to complete training.	The trainer will listen to investigators take calls during the week of field training. Three calls will be evaluated at random using an audit rubric that is subdivided by each required skill. Points are deducted for any procedural steps missed during the call. The instructor will average the three audits to determine if the investigator is able to transition from training into their job role.

8. Performance Objectives

Investigators are expected to complete all eLearning courses with a passing grade of 80% or higher. In addition to the required eLearning courses, investigators will be audited on three of their calls, selected at random. Investigators must score an average of 80% or higher on call audits to complete their training. *See Appendix C for Call Audit Rubric.*

Goal Analysis	Subordinate Skill	Objective
1. Explain the different types of fraud/scams and how they work.	1.1 Differentiate between types of fraud/scams (CR). 1.2 Determine which probing questions to ask for each type of fraud/scam (CR).	1.1 Identify the fraud scam type. (B/O). 1.2 Investigator will be able to ask the appropriate probing questions to identify fraud/scam type (O).
2. Identify the customer's initial issue or problem. Determine preliminary fraud scam type.	2.1 Receiving a call (CN), investigator will actively listen to the victim explain issues or problems(B) to determine the type of fraud scam (CR). 2.2 Based on information provided, the investigator will determine what additional information is needed to ensure they have all the information needed to review the account (CR).	2.1 Actively listen to victim and take note of the information being provided and determine the preliminary fraud scam type. (O). 2.2 Investigator will determine which additional probing questions are needed (O).
3. Ask additional probing questions to conduct review of account activity.	3.1. Ask victim probing questions to gather additional information needed to review the account (B). 3.2. Review account activity, notations, and alerts on account to compare it with the information provided by customer (B).	3.1.1 Investigator will ask appropriate probing questions to review accounts (O). 3.2.1 Determine the fraud scam type (O).
4. Determine what information has been compromised by fraudster.	4.1. Verify activity and determine what information has been compromised to ensure the account is secured (CR). 4.2 Ensure accounts are currently secured to prevent any further damage (CR).	4.1.1 Identify and verify with customer what information is compromised (O). 4.2.1 Secure victim's accounts (if not done already) (O).
5. Determine what if any fraud activity occurred on victim's account.	5.1 Review account transactions with victim to determine what if any fraud occurred to file fraud claim if needed (CR). 5.2 File fraud claim (B).	5.1.1 Investigator determine which transactions are fraudulent (O). 5.2.1 Recover lost funds for victim (O).
6. Provide appropriate educational information to victim to protect their Personal Identification Information and accounts.	6.1 Advise/explain the fraud scam scenario scheme and how it affects victims (B). 6.2 Educate victims on how to keep personal identification information secure (B). 6.3 Provide customers with additional tools to prevent them from falling victim to future fraud scam attempts. (B).	6.1.1 Investigators will use correct verbiage and guidance to explain how fraud scams work to customers (O). 6.2.1 Advise on how to keep PII and devices secured (O). 6.3.1 Send Identity Theft brochure to victims (B/O).
7. Have victim close and open new accounts and/or change login credentials if needed.	7.1 Transfer customers with compromised accounts to appropriate department to close/open new accounts and change login credentials (B).	7.1.1 Initiate transfer to appropriate department to open new accounts (O).

9. Design Evaluation Chart

Investigators are expected to complete all eLearning courses with a passing grade of 80% or higher. In addition to the required eLearning courses, investigators will be audited on three of their calls, selected at random. Investigators must score an average of 80% or higher on call audits to complete their training. *See Appendix C for Call Audit Rubric.*

Goal Analysis	Subordinate Skill	Objective	Evaluation
1. Explain the different types of fraud/scams and how they work.	1.1 Differentiate between types of fraud/scams (CR). 1.2 Determine which probing questions to ask for each type of fraud/scam (CR).	1.1 Identify the fraud scam type (B/O). 1.2 Investigator will be able to ask the appropriate probing questions to identify fraud/scam type (O).	Elearning with 11 question assessment that must be passed with 80% or higher). Mock call role plays scenarios to assess any gaps in procedural skills before performing job duties. (Trainer will determine if trainee is able to proceed with fields: Taking calls in training environment with Mentor side by side to assist with questions).
2. Identify the customer's initial issue or problem. Determine preliminary fraud scam type.	2.1 Receiving a call (CN), investigator will actively listen to the victim explain issues or problems(B) to determine the type of fraud scam (CR). 2.2 Based on information provided, the investigator will determine what additional information is needed to ensure they have all the information needed to review the account (CR).	2.1 Actively listen to victim and take note of the information being provided and determine the preliminary fraud scam type (O). 2.2 Investigator will determine which additional probing questions are needed (O).	Call evaluation. The trainer will listen to trainee take calls. Three calls will be evaluated with a rubric that is subdivided by each required skill. Points are deducted for any procedural steps missed during the call. The evaluation scores will be average. Trainees must score 80% to pass.
3. Ask additional probing questions to conduct review of account activity.	3.1. Ask victim probing questions to gather additional information needed to review the account (B). 3.2. Review account activity, notations, and alerts on account to compare it with the information provided by customer to determine the fraud scam type (B).	3.1.1 Investigator will ask appropriate probing questions to review accounts (O). 3.2.1 Investigators will use systems to review activity conducted on the account (B). Determine the fraud scam type (O).	See above Table 1. Evaluation: Trainer will determine if the trainee actively listened to victim to ask the appropriate probing questions. Ensure the trainee is not asking the victim to repeat information previously provided. Actively taking notes. Reviews accounts appropriately and thoroughly to verify information matches activity.
4. Determine what information has been compromised by fraudster.	4.1. Verify activity and determine what information has been compromised to ensure the account is secured (CR). 4.2 Ensure accounts are currently secured to prevent any further damage (CR).	4.1.1 Identify and verify with customer what information is compromised (O). 4.2.1 Secure victim's accounts (if not done already) (O).	See above Table 1. Evaluation: Reviews accounts appropriately and thoroughly to verify information matches activity. Verifies security of victims' assets. Informs victim of any pertinent information regarding accounts and assets.

5. Determine what if any fraud activity occurred on victim's account.	5.1 Review account transactions with victim to determine what if any fraud occurred to file fraud claim if needed (CR). 5.2 File fraud claim (B).	5.1.1 Investigator determine which transactions are fraudulent (O). 5.2.1 Recover lost funds for victim (O).	Evaluation: Trainer will review call to verify investigator followed all procedural steps correctly. Verbally verifies all activity on account to determine if fraud activity occurred. Files appropriate claims following correct procedures, read disclosures, and inform the customer of pertinent information regarding the claim process.
6. Provide appropriate educational information to victim to protect their Personal Identification Information and accounts.	6.1 Advise/explain the fraud scam scenario scheme and how it affects victims (B). 6.2 Educate victims on how to keep personal identification information secure (B). 6.3 Provide customers with additional tools to prevent them from falling victim to future fraud scam attempts. (B).	6.1.1 Investigators will use correct verbiage and guidance to explain how fraud scams work to customers (O). 6.2.1 Advise on how to keep PII and devices secured. (O). 6.3.1 Send Identity Theft brochure to victims (B/O).	See above Table 1. Evaluation: Evaluate if appropriate information was provided to the victim. Any forms or brochures needed were correctly sent.
7. Have victim close and open new accounts and/or change login credentials if needed.	7.1 Transfer customers with compromised accounts to appropriate department to close/open new accounts and change login credentials (B).	7.1.1 Initiate transfer to appropriate department to open new accounts (O).	See above Table 1. Evaluation: Followed correct procedures to assist the victim with getting to the correct specialist to finish completing account security procedures.

10. Instructional Strategy

Content Presentation and Student Participation Learning Components for Cluster One:

Performance Objectives Subordinate to Main Step 1:

Subordinate Skill 1.1: Differentiate between types of fraud/scams (CR).

- **Objective 1.1.1:** Identify the fraud scam type. (B/O).

Subordinate Skill 1.2: Determine which probing questions to ask for each type of fraud/scam (CR).

- **Objective 1.1.2:** Investigator will ask the appropriate probing questions to identify fraud/scam type (O).

Student Grouping and Media Selection:

Student Grouping: Self-Paced independent learning

Media Selection: e-Learning course that includes the following:

- Short videos: Cybersecurity overview, example scenario of how victims fall pretty to scams, example call scenario for providing verbiage to victims.
- Downloadable job-aids for verbiage.
- Intranet procedural manual page.
- Intranet pages on security awareness investigators can bookmark.
- FBI scam safety and FTC fraud reporting webpage.

Pre-Instructional Activities:

Can anyone tell me what they think social engineering is?
Can anyone name a type of cyber scam?
Can anyone give me an example of a cyber scam and explain how it works?
Has anyone personally experienced or know anyone who has experienced a scam of any kind?
(Instructor will engage learners by asking the questions above. Call on volunteers to answer the questions. Have an open discussion about social engineering. Discuss Cyber scams and fraud trends learners are familiar with or have experienced personally. If instructor has a personal experience, they will share their experience with learners).

Today we are going to learn some of the core skills needed for your job role as security investigators. Before we really start learning the technical and procedural skills you will need. There is an eLearning that you will take that provides an overview of your job role. It explains the different types of cyber scams and how they work. It outlines the red flags you will look for when assisting customers, the right probing questions to ask for each scam type, education information and verbiage you can use for your calls. There are several job aids that will be provided in the eLearning that you can save for use later. You will have an assessment once you are finished. Please send me a message when you have finished so that I can provide you a link to take the assessment. You must pass the assessment with an 80% or higher. What questions do we have so far?

Content Presentation:

The instructor will demonstrate and assist investigators on how to navigate their learning profiles to locate the eLearning course. Investigators will work independently on an eLearning course that should take approximately 30 minutes. The eLearning will cover what cyber scams are, how they occur, and the red flags associated with each. It will provide investigators with the appropriate probing questions to ask for each scam. It will also provide methods and verbiage to use to educate on prevention and protection methods to help account holders from falling victim again in the future.

Section One: What is Social Engineering
Section Two: Types of Social Engineering Scams
Section Three: How it Works
Section Four: How to Identify Customers who are Scam Victims
Section Five: How Does Social Engineering Affect Victims
Section Six: Educating Customers on Ways to Protect and Prevent Being a Victim
Section Seven: Quiz
Section Eight: Summary

Scam Trend Scenario Types Covered:

1. Phishing	5. Messages from Government Entities
2. Vishing	6. Problems with Accounts
3. Smishing	7. A Friend or Family Member in Need
4. The Contest Winner	8. Tech Support Imposters

Practice Items and Activities:

1. Interactive Graph
2. Four example call scenarios that will assess investigator's ability to determine scam type.
3. Link to sign up for Security Fraud Community.
4. Handouts and job aids for learners to download and save for future use.
5. Knowledge check of 11 questions at the end of the eLearning.
6. Gamified assessment with six call scenarios that will test basic skills learned in eLearning.

Videos:

Explanation social engineering
Real life scenario of Vishing
Mock call animated scenario

Determining Scam or Fraud Call Scenario Activity:

1. ATO: Online loan victim.	2. Smishing: Malicious link.
3. Check: Large check dep with an immediate attempted Western Union withdraws.	4. Mule calling to report fraudulent transfer received.

Gamified Assessment:

Assessment gamification assessment will consist of six scam scenarios. The storyline for the player: They are being recruited as an investigator for an elite security force. To become an investigator, they have six missions to complete. The mission is to help each potential scam victim by identifying the red flags, the right probing questions to ask, and appropriate prevention education. For each mission, they are presented with a comic strip of a scam scenario. They will use the comic to determine the type of scam. They will have to answer three - five multiple-choice questions permission. The game is currently set up so that if the question is answered incorrectly, it prompts with a mission failed/try again. They can keep trying till they get the answer right to move to the next question/mission. Once all the missions/scenarios are completed, the player is presented with their security investigator badge.

Feedback:

Investigators will receive immediate feedback for *each* knowledge check activity completed throughout eLearning. Instructor will be able to see which questions were missed on each attempt. Knowledge checks will allow investigators multiple attempts until completed correctly. The eLearning knowledge check and gamified assessment must be passed with a score of 80% or higher. Feedback will also be provided by the instructor based on assessment results. Instructor will be able to see which questions were missed on *each* attempt.

Content Presentation and Student Participation Learning Components for Cluster Two:

Performance Objectives Subordinate to Main Step 2 through 7:

Note: Cluster two is the design for mock role-play call scenarios that will be added to the end of current curriculum model for different call types.

Student Grouping and Media Selection:

Student Grouping: Both entire class as well as Individual Investigator paired with Instructor.
Media Selection: Instructor led Mock Call Scenario/Role Play, observation, and Feedback.

NOTE:

For this activity the trainer will need to review mock call scenario examples prior to the lesson to ensure scenarios are up to date. Make modifications as needed based on fraud scam trends to ensure investigators are practicing accurate job skills performed in real world setting. Provide an example for each of the main fraud scam trends investigator might encounter.

- The instructor will use a job aid previously provided to investigators with different verbiage or scripts they can use while assisting victims.
- Be sure examples provide additional information for follow up probing questions investigators come up with to ask customer to review the account.

NOTE: *This activity will be repeated in sequential order for each call scenario type at the end of that call type's lesson. It will be used to assess skills transfer by instructor to identify any gaps that may need to be re-reviewed.*

Performance Objectives Subordinate to Main Step 2:

Subordinate Skill 2.1: Receiving a call (CN), investigator will actively listen to the victim explain issues or problems(B) to determine the type of fraud scam (CR).

- **Objective 2.1.1:** Actively listen to victim and take note of the information being provided to determine potential scam type.

Subordinate Skill 2.2: Based on information provided, the investigator will ask additional probing questions to ensure they have all the information needed to review the account (CR).

- **Objective 2.2.1:** Determine additional probing questions needed to gather more information for review of account.

Pre-Instructional Activities:

Earlier, you completed an Elearning that explained what social engineering is and the different types of social engineering scams that customers may unknowingly encounter. Who can name some of the types of scams examples that were discussed? (Allow volunteers to provide examples discussed in the Elearning). Does anyone remember some of the probing questions go with each specific type of scam? (Allow volunteers to discuss or have a group discussion about the probing questions associated with each scam type). Now we are going to look at a few examples of Mock account scenarios. I am going to give you a synopsis of why the customer's account access has been restricted. What I'd like for you to do is based on the scenario information provided, I'd like you to write what type of scam you believe the customer fell victim too. Once you have determined the scam type, I'd like for you to list any additional probing questions you think are needed to verify the scam. I will give you 10 minutes for each scenario to write out your answers, we will discuss what everyone came up with afterwards. I have several scenarios that we will go over.

Content Presentation:

Instructor will display power point slides with mock scam call scenario annotations. Scenarios will provide some basic detailed information a customer might provide up front when calling regarding activity that has occurred due to a potential scam. Instructor will read the scenario to the training class. Allow adequate time for everyone to determine scam type and additional probing questions.

Example: Online Loan Scam Victim:

Customer Mr. Smith is calling because he is not able to access his account. He advises that he is very upset because he is at the store attempting to get a Money Order from a rental agency to pay his deposit and first month's rent to secure a new apartment. He says his card is not working and he doesn't understand why. He knows he has money in the account because he just received a deposit from a loan, he was approved for that he applied for online earlier today to get this department. He also says he is frustrated because this has been a very long process for him. The loan company made him do several things to verify his account to get approved for this loan. He has been at this store for a while and is ready to just to get the keys to his new apartment so he can relax.

Correct Additional Questions:

1. Can you verify the name of the loan company?
2. Did you provide your login credentials to the third party or did the application or approval email prompt for you to login to your account for verification purposes?
3. Can you verify the amount of the loan they stated you were approved for?
4. Did they say how the loan proceeds would be deposited?
5. When you say the loan company had you do several things to verify your account, can you provide a little more information about what they needed you to do?

Example Call Types:

1. ATO (online loan, impersonator, Tech support, or phishing)	2. IDT (new account restricted)
3. Check (social media, romance scam, or sweepstakes)	4. Mule (friend/family member, provisional credit)

Example Scam Scenario Types: *Other call scenario examples that will be simulated in each lesson pertaining to call types.*

1. Romance Scam	5. Tech Support/Computer Virus
2. Social Media Scam	6. Imposter/Impersonator
3. Check Scams	7. Mule: Friend or Family Member in Need
4. Job Scam	8. Phishing, Smishing and Vishing

Practice Items and Activities:

1. List specific type of scam.
2. List additional probing questions investigator would need to ask customer to gather additional information to confirm suspected fraud scam type.
3. Begin practice taking notes that will be used to place on member's account.

Feedback:

Review and discuss each scenario as a group. Decide on the preliminary scam type and the additional probing questions that are needed to gather more information to review the account activity.

- If needed, advise the investigators of the potential scam type associated with the scenario as well as the correct probing questions investigators would ask. Explain why or how they would determine this information.

- NOTE: Be sure to have an open discussion about any wrong scam types identified as well as probing questions. Discuss why those responses are incorrect. Provide tips or ways investigators can easily identify scam types.
  - EX: Review the alert notations – comments will provide investigators activity or call scenario type.

Performance Objectives Subordinate to Main Step 3:

Subordinate Skill 3.1: Ask victim probing questions to verify all Personal Identification and/or account/login information has been completed (B).

- Objective 3.1.1: Investigator will ask appropriate probing questions to review accounts (O).

Pre-Instructional Activities:

Now that we have listened to customers explain their initial issues, we have made a preliminary decision on the type of fraud scam as well as decided if any and what additional questions may be needed to gather more information prior to further reviewing the account activity.

So, what we will do next, is practice asking the customer additional probing questions to ensure we have all the information we need to review the account activity in comparison to this information we now have. We are going to take turns asking one of the probing questions we came up with to see what additional information the customer provides to us for this scenario.

Content Presentation:

Instructor will continue to display power point slides associated with mock scam call scenario annotations with the basic detailed information a customer might provide up front when calling regarding activity that has occurred due to a potential scam. Instructor will have volunteers or will go around the room having each investigator ask at least one additional probing question.

Example: Online Loan Scam Victim Additional information for probing questions scenario continued:

Probing Question with Additional Information:

1. Can you verify the name of the loan company?
    - Mr. Smith: Yes, it was Rapid Fast Loans Inc.
2. Did you provide your login credentials to the third party or did the application or approval email prompt for you to login to your account for verification purposes?
    - Mr. Smith: The application asked me to log into my account to verify it. Then the representative called me. He said he also needed to send me a code. They were going to make a test deposit that I needed to send back to them to verify my account before they deposited the loan.
3. Can you verify the amount of the loan they stated you were approved for?
    - Mr. Smith: I was approved for $3000.00.
4. Did they say how the loan proceeds would be deposited?
    - Mr. Smith: They just said it was a direct bank deposit.
5. When you say the loan company had you do several things to verify your account, can you provide a little more information about what they needed you to do?
    - Mr. Smith: They said they made a test deposit to my account and in order to finish the verification process I needed to send the funds back to them through cash app. This would also verify and set up my monthly auto payments. I told them I did not have cash app. They made me go purchase these gift cards and make these deposits at this ATM in Walmart. They said this is how I would have to make my payments.

Example Call Types:

1. ATO (online loan, impersonator, Tech support, or phishing)	2. IDT (new account restricted)
3. Check (social media, romance scam, or sweepstakes)	4. Mule (friend/family member, provisional credit)

Example Scam Scenario Types: *Other call scenario examples that will be simulated in each lesson pertaining to call types.*

1. Romance Scam	5. Tech Support/Computer Virus
2. Social Media Scam	6. Imposter/Impersonator
3. Check Scams	7. Mule: Friend or Family Member in Need
4. Job Scam	8. Phishing, Smishing and Vishing

Practice Items and Activities:

1. Practice asking probing questions.
2. Practice forming account notation to be left on customer's profile.

Feedback:

Review and discuss the new additional information that has been provided by the customer. Discuss whether the new information has changed their preliminary decision of the fraud scam type. Discuss any feedback for question

strategies: questions asked in an open-ended non leading manner? Tone, inflection, active listening skill used appropriately.

- Be sure to have an open discussion about any wrong scam types identified as well as the proper way to word and ask probing questions. Discuss errors made and offer corrections.

Performance Objectives Subordinate to Main Step 3:

Subordinate Skill 3.2: Review account activity, notations, and alerts on account to compare it with the information provided by customer to determine the fraud scam type (B).

- Objective 3.2.1: Investigators will use systems to review activity conducted on the account (B). Determine the fraud scam type (O).

(Portions of this section has been scrubbed of detailed information. Brief generalized idea of the instructional activities has been provided.)

The instructor will demonstrate how to navigate the system in detail to review an account based on the information provided and the restrictions placed.

Pre-Instructional Activities:

So far, we have practiced the basic call skills and procedures needed to gather information to make a preliminary decision of the fraud scam type. Now that we have this information, we will need to conduct a review of the account and activity to verify if this information matches the activity. Why do you think it is important to compare the information provided by the member to the activity seen on the account?

It is important to compare the activity with the information provided by the member to verify the correct scam type so that we can provide the right education on protection and prevention as well as make sure all the customers' assets are secured.

Content Presentation:

The instructor will prepare examples of accounts for each scam type that matches the scenarios listed below. Examples will be used to show investigators how to review alerts, notes, and double check activity on account. The instructor will demonstrate reviewing an account activity based on information provided. Discuss what information is discovered based on comparison of information and activity.

NOTE: Instructor will reach out to SMEs or current investigators to have them provide examples for use.

Example: Online Loan Scam Victim Additional information for probing questions scenario continued:

(This information has been Scrubbed. The example accounts would match the scam scenario and mock information created for the role play activity.)

Example Call Types:

1. ATO (online loan, impersonator, Tech support, or phishing)	2. IDT (new account restricted)
3. Check (social media, romance scam, or sweepstakes)	4. Mule (friend/family member, provisional credit)

Example Scam Scenario Types: *Other call scenario examples that will be simulated in each lesson pertaining to call types.*

1. Romance Scam	5. Tech Support/Computer Virus
2. Social Media Scam	6. Imposter/Impersonator
3. Check Scams	7. Mule: Friend or Family Member in Need
4. Job Scam	8. Phishing, Smishing and Vishing

Practice Items and Activities:

1. Practice navigating the systems to locate and review notes as well as alerts.
2. Practice navigating reviewing activity history.
3. Determine fraud scam type accurately.
4. Practice forming account notation to be left on customer's profile.
5. Practice asking probing questions.

Feedback:

Discuss and review different systems used to review the activity. Ask verbal recall questions to test investigators knowledge or memory of the different systems and how to navigate each one to locate the information they need to review. Have them describe what information they are reviewing and why. Have an open discussion about discrepancies or errors that are made. Provide feedback to investigators as they demonstrate procedural steps taken to navigate systems and review activity. Discuss any mistakes they made. Answer any questions that may come up. Ensure all investigators can complete procedural steps before moving to the next session.
NOTE: Some of the procedures can be performed several different ways. Verify the investigator can navigate efficiently to the location in the system they need to, they are reviewing the right activity and can accurately describe or verify what the activity is that is reviewed.

Performance Objectives Subordinate to Main Step 4 and 5:

Subordinate Skill 4.1: Verify activity with customer and determine what information has been compromised to ensure the account is secured (CR).

- Objective 4.1.1: Identify and verify what information is compromised (O).

Subordinate Skill 4.2: Ensure accounts are currently secured to prevent any further damage (CR).

- Objective 4.2.1: Ensure proper steps are taken to secure victim's accounts (if not done already) (O).

Subordinate Skill 5.1: Review account transactions with victim to determine what if any fraud occurred to file fraud claim if needed (CR).

- Objective 5.1.1: Investigators determine which transactions are fraudulent (O).

Subordinate Skill 5.2: File fraud claim (B).

- Objective 5.2.1: Recover lost funds for victim (O).

(Portions of this section has been scrubbed of detailed information. Brief generalized idea of the instructional activities has been provided.)

The instructor will also provide a mock call scenario example to talk through procedural steps investigators will take next. The instructor will demonstrate steps and systems investigators will take to verify activity with the victim once they have reviewed the account. The instructor will also explain and demonstrate procedural steps for securing or actioning the account. Group discussion about what questions should be asked to verify any information compromised.

Pre-Instructional Activities:

Now that we have reviewed the accounting activity and compared it to the information provided by the victim, we need to confirm any activity that is still in question. We would need to have the victim verify if they conducted or are aware of any activity or transactions that were not previously confirmed. You will file a fraud claim for any activity the victim is reporting as fraud. Before completing the claim, be sure to read any disclosures for the claim to the victim. It

is important to provide accurate information regarding the claim process to victims. Otherwise, we could be in violation of federal regulations and compliance which can lead to fines. So, I just want to say this again. We need to ensure we are filing claims as soon as the victim reports any kind of fraud. We must ensure we are providing the correct information regarding the claim process and recovery of funds. (*This section has been modified, reworded, and partially scrubbed due to internal confidential information provided regarding compliance and regulations for claim processes and procedures*).

Content Presentation:

The instructor will prepare examples of accounts for each scam type that matches the scenarios listed below. Examples will be used to show investigators how to verify activity and what information has been compromised with the victim using the correct probing questions. The instructor will demonstrate how to action the account correctly to ensure it is secure. The instructor will talk through a real-world mock call scenario with the appropriate probing questions while demonstrating the steps investigators will take to ensure the account is secure.

NOTE: Instructor will reach out to SMEs or current investigators to have them provide examples for use.

Example: Online Loan Scam Victim Additional information for probing questions scenario continued:

(This information has been Scrubbed. The example accounts would match the scam scenario and mock information created for the role play activity.)

Example Call Types:

1. ATO (online loan, impersonator, Tech support, or phishing)	2. IDT (new account restricted)
3. Check (social media, romance scam, or sweepstakes)	4. Mule (friend/family member, provisional credit)

Example Scam Scenario Types: *Other call scenario examples that will be simulated in each lesson pertaining to call types.*

1. Romance Scam	5. Tech Support/Computer Virus
2. Social Media Scam	6. Imposter/Impersonator
3. Check Scams	7. Mule: Friend or Family Member in Need
4. Job Scam	8. Smishing and Vishing

Practice Items and Activities:

1. Demonstrate how to verify fraud activity on the account.
2. Roleplays probing questions used to confirm fraud activity with victim.
3. Role plays probing questions used to confirm what information is compromised.
4. Practice navigating system to secure accounts. Step by step procedure to restrict or grant access.
5. Practice filing fraud claim.
6. Reading claim disclosures to victim.

Feedback:

Discuss and review different systems used to secure accounts. Ask verbal recall questions to test investigators knowledge of which probing questions to ask for each scam scheme. Have them explain why they chose the probing questions provided. Provide feedback to each investigator as they demonstrate procedural steps for securing accounts, filing fraud claims, and verifying what information is compromised. Have them demonstrate the step-by-step procedural actions to secure account. Have an open discussion about discrepancies or errors that are made.

NOTE: Some of the procedures can be performed several different ways. Verify the investigator can navigate efficiently to the location in the system they need to, they are reviewing the right activity and can accurately describe or verify what the activity is that is reviewed.

Performance Objectives Subordinate to Main Step 6:

Subordinate Skill 6.1: Advise/explain the fraud scam scenario scheme and how it affects victims (B).

- **Objective 6.1.1:** Investigators will use correct verbiage and guidance to explain how fraud scams work to customers (CR).

Subordinate Skill 6.2: Educate victims on how to keep personal identification information (CR).

- **Objective 6.2.1:** Secure victims accounts (if not done already) (CR).

Subordinate Skill 6.3: Provide customers with additional tools to prevent them from falling victim to future fraud scam attempts (B).

- **Objective 6.3.1:** Send Identity Theft brochure to victims (B/O).

(Portions of this section has been scrubbed of detailed information. Brief generalized idea of the instructional activities has been provided.)

Pre-Instructional Activities:

Once we have reviewed the account, verified all activity, and filed any necessary fraud claims, can anyone tell what they would do next?

Next, we will advise of why the activity caused the restriction on the account. We will also need to explain the scam scheme so that the victim fully understands so they don't fall victim again in the future. Would anyone like to pick a scam trend to explain how it works and how victims fall prey to it?

- Pick a volunteer to explain a scam trend. If no one volunteers, the instructor should pick a scam trend as an example.
- Instructor will assign each investigator a scam to practice explaining. Have each investigator explain their scam trend to the class as if they were talking to a victim.

Great! Now that we have explained how the scam happens, we need to educate victims on ways to keep their personal and account information secure.

(This portion has been scrubbed: Instructor will repeat same practice activity used to explain scam scheme).

Would anyone like to take a guess at what they should do after they have educated the victim?

- Pick a volunteer to explain the next procedural step. If no one volunteers, the instructor can call on someone to explain or explain themselves.

Once you have educated the victim you will want to provide them with any resources, they need to protect their personal information. There are several different resources we have that we can offer to send or direct them to. Let's look at the different resources and how we can provide them to victims.

- Instructor will demonstrate how to send the ID Theft brochure to victims.
- Provide external resources victims can use to report scams and protect their personal information. Review each source and how it will assist victims.

(This portion has been scrubbed: Instructor will demonstrate procedural steps for sending/providing resources to victims)

Content Presentation:

The instructor will prepare examples of accounts for each scam type that matches the scenarios listed below. Examples will be used to show investigators how to review alerts, notes, and double check activity on account. The instructor will demonstrate reviewing an account activity based on information provided. Discuss what information is discovered based on comparison of information and activity.

NOTE: Instructor will reach out to SMEs or current investigators to have them provide examples for use.

Example: Online Loan Scam Victim Additional information for probing questions scenario continued: *(portions of this example have been scrubbed).*

Example verbiage:

"I understand you are frustrated and confused Mr. Smith. I will be honest: based on the information you provided and what I have confirmed in our bank systems, you are a victim of an online loan scam. You provided your login credentials to a Scammer. The scammer accessed your account and filed a false fraud claim, which issued your account a provisional credit (temporary credit). Then they had you transfer the funds to their Cash App account.

I have submitted a request to cancel this false claim. Unfortunately, that means the provisional credit issued to the account will be debited back out of your account, leaving a negative balance. You will be responsible for the balance owed because you transferred the funds from the account, which is how these scams work.

These scammers manipulate their victims into providing bank information, such as account numbers, login credentials, or card information. They have their victims assist with the activity, which usually involves transferring the funds out, which causes the victim to be responsible for the balance, and the scammer gets the money.

Going forward, just be mindful of keeping your login credentials secure. No one, not even family members or spouses, should have access to your login credentials. That is only for your use. For security purposes, we do not even have access to that information. If anyone requests to verify your account by logging in or asking to deposit funds for any reason, this is typically a red flag for a fraud scam. Lending companies typically verify bank information with a statement.

I am going to send you a copy of our Identity Theft brochure. Since the loan application requested all your personal identification information, you will want to take additional measures to safeguard your identity. This brochure provides good tips on protecting yourself going forward. There's a checklist of steps and tips for safeguarding your identity. I highly recommend contacting the different credit bureaus to request a freeze and for fraud alerts to be placed on your credit profile. This will help with any potential fraudulent lending applications or accounts being opened in your name fraudulently.

If you are unsure if something is legitimate, you can call us at any time. There are representatives here 24/7 for assistance. We are happy to help verify or answer any questions you have. We want to help protect you. I am going to transfer you over to a fraud specialist so they can assist you with securing your accounts and getting your access back. Before I do, do you have any questions or anything I may assist with?"

Example Call Types:

1. ATO (online loan, impersonator, Tech support, or phishing)	2. IDT (new account restricted)
3. Check (social media, romance scam, or sweepstakes)	4. Mule (friend/family member, provisional credit)

Example Scam Scenario Types: *Other call scenario examples that will be simulated in each lesson pertaining to call types.*

1. Romance Scam	5. Tech Support/Computer Virus
2. Social Media Scam	6. Imposter/Impersonator
3. Check Scams	7. Mule: Friend or Family Member in Need
4. Job Scam	8. Smishing and Vishing

Practice Items and Activities:

1. Practice explaining how different types of fraud scams occur and how victims fall prey.
2. Role-play mock call scripts for account security and education verbiage.
3. Work on creating or modifying scripts into their words.
4. Investigators demonstrate procedural steps taken to send ID Theft brochure.
5. Review external sources provided to victims.

Feedback:

Discuss and review different systems used to explain scams. Ask verbal recall questions to test investigators knowledge or memory of the different systems and how to navigate each one to process procedural steps. Have them describe other ways they can provide education or assist victims with protecting themselves from future scams. Provide feedback to investigators as they demonstrate procedural steps taken to navigate systems and review activity. Discuss any mistakes they made. Answer any questions that may come up. Ensure all investigators can complete procedural steps before moving to the next session.

NOTE: Some of the procedures can be performed several different ways. Verify the investigator can navigate efficiently to the location in the system they need to, they are reviewing the right activity and can accurately describe or verify what the activity is that is reviewed.

Performance Objectives Subordinate to Main Step 7:

Subordinate Skill 7.1: Verify activity and determine what information has been compromised to ensure the account is secured.

- Objective 7.1.1: Identify what information has been compromised to ensure the account is secured (CR).

(Portions of this section has been scrubbed of detailed information. Brief generalized idea of the instructional activities has been provided.)

The instructor will demonstrate how to determine what information provided by the member contradicts activity conducted on the account. Instructor will also explain how to determine what activity needs to be verified/re-verified.

Pre-Instructional Activities:

Once you have completed all your procedures. The last thing you will need to do is transfer the victim to a fraud specialist. Can anyone tell me why we are transferring the victim to a fraud specialist?

We need to transfer them so the specialist can assist them with changing their login credentials and opening new accounts. Be sure to advise the victim that you will be transferring them to another specialist and what their next steps will be. Can anyone explain the steps you will take to initiate the transfer?

- Pick a volunteer to explain the next procedural steps. If no one volunteers, the instructor can call on someone to explain or explain themselves.
- The instructor will also provide a demonstration.

Content Presentation:

The instructor will demonstrate procedural steps investigators will take in systems to initiate a transfer.

Examples:

(This information has been Scrubbed. The example accounts would match the scam scenario and mock information created for the role play activity.)

Practice Items and Activities:

1. Instructor will have each investigator demonstrate procedural steps for initiating a transfer.

Feedback:
Discuss and review different systems used to initiate call transfer. Ask verbal recall questions to test investigators knowledge on what they should advise victims when transferring. Provide feedback to investigators as they demonstrate procedural steps taken to navigate systems and review activity. Discuss any mistakes they made. Answer any questions that may come up. Ensure all investigators can complete procedural steps before moving to the next session.

NOTE: Some of the procedures can be performed several different ways. Verify the investigator can navigate efficiently to the location in the system they need to, they are reviewing the right activity and can accurately describe or verify what the activity is that is reviewed.

11. Implementation Plan

The module will be test piloted in several training classes and by a small group of tenured investigators. Informal feedback will be gathered by the instructor immediately after completing the assessment. Formal feedback will be collected through a weekly training survey.

- The modules will be piloted with 3-4 training classes as well as a small group of tenured investigators.
- Each participant will work alone, but assistance will be provided by an instructor if needed.
- Investigators will be given a total of 60 minutes to complete both the eLearning and gamified assessment.
- Implementation of this module will be considered successful if the testers are able to complete the module with an evaluation score of 80% or higher on the first try.

After feedback is provided by learners, tenured investigators, and leadership any revisions needed will be made prior to implementation.

1. Organizational Approval
    - Identify key stakeholders and committees needed to approve the initiative and policy.
        - Security Leadership, Security Training Leadership, Projects and Process Improvements, and Design Team.
    - Obtain buy-in; attend meeting agendas for approval.
        - Update various key stakeholders and leadership.
        - Approve policy - Security Leadership
    - Finalize implementation date – "Go Live" date.
        - Security training revamp
    - Implementation plan – Projects and Process Improvements
        - Finalize implementation date – SME and training pilot.
        - Finalize implementation date – "Go Live" date.
            - Security training revamp

2. Documents and Materials Procurement
    - Develop training communication materials.

    Develop training materials:

    - Cluster One: eLearning and gamified assessment will be added to the beginning of the existing curriculum. This will be a self-paced module that will be integrated into day one of the instructor led training.
        - Articulate Rise 360 will be used to construct the eLearning module.
        - Existing manuals, job aids, and IDer's job experience will be used to compile curriculum.
        - External resources approved by Security Leadership will be used to comprise victim education information and resources.
        - Recorded calls from previous investigators will be reviewed to assist with writing mock call scenario examples.
        - Links for Security ENET pages, manual links and job aids will be embedded in the course for learners to save for references.
        - Rise eLearning will be uploaded to a learning database located on the ENET that learners will have access to for course completion.

    - Cluster Two: Mock Role-Play call scenarios will be integrated at the end of each training module pertaining to different call types Days 2-5.
        - Genially will be used to design the gamified assessment.

    - Canva will be used to create all the graphics and detailing for gamification assessment and uploaded to Genially.
    - Vyond will be used to create the Mock Call video scenarios for the assessment.
    - Recorded calls from previous investigator will be reviewed and selected as the audio for the videos. (names and personal identification information will be scrubbed). One call selected for each scam type. (*Course design: AI and abbreviated call scenarios were used)*
        - Pilot phase: Total of six call types will be used. The number of scenarios may change based on feedback and data collected after completion of the pilot and SME testing.
    - Learners will be provided with link a link for the assessment during pilot phase with the protected password by the training instructor.
        - SME testing- IDer will provide the link and password via email.
- Design course evaluations and determine all methods for all feedback assessments.
    - Schedule meetings with PPI analysts for feedback reviews.

3. Technology and Software
    - Learners will be provided with or will already have resources and technology tools needed.
    - Work with IT management to have materials available via ENET learning database prior to the "Go Live" date.
        - Existing manuals, job aids, and IDer's job experience will be used to compile curriculum.
        - Recorded calls of previous investigators will be reviewed to assist with writing mock call scenario examples.
        - Rise eLearning will be uploaded to a learning database located on the ENET that learners will have access to for course completion.
        - If successful, gamified assessment will be uploaded to ENET learning database.
            - (It has not been uploaded due to concerns with accessibility of all employees).

4. Communication Plan
    - Identify and set up briefings for project team.
    - Establish communication loop between ID and security supervisors regarding SME test piloting.
        - Establish participants, dates, and times for SME pilots to be conducted.
        - Instruction emails and reminders sent to SME pilot participants leading up to pilot testing.
    - Create e-mails communication loops with all stake holders to be sent out periodically leading up to SME pilots with dates and instructions.
    - Create e-mails communication loops to be sent out periodically leading up to the "Go Live" date.
    - Meet with security training team stakeholders.
        - Ensure curriculum, job aids and resources are up to date and consistent.
        - Ensure all materials are accessible based on organizational standards.
    - Assign ISD, project manager and supervisor for questions/issues during implementation and the following month.

5. Educations & Training Plan
    - Identify trainers and schedule train-the-trainer sessions (back up trainers as ID is the trainer).
        - Familiarize trainer with training content and tools (Systems and access, troubleshooting instructions, and training competency).
    - Verify training dates, times, and locations. Set training schedules.
    - Schedule meetings with leadership and project management teams.

6. Two Weeks Before Roll Out – SME Test Pilot Dates
    - Send a reminder e-mail to all trainers and leadership to ensure all access has been granted.
    - Check with PPI for possible questions/issues that may have arisen. Technical issues with enrollment and access errors.

- Verify any reporting discrepancies, if any, have been fully resolved.

Two Weeks Before Roll Out – "Go Live" Date

- Send e-mail reminders to trainers and leadership regarding feedback.
- Check with ISD and trainer regarding possible questions/issues that may have arisen. Technical issues with enrollment and access errors.
- Verify any reporting discrepancies, if any, have been fully resolved.

7. Follow-up and Evaluation (*see detailed Evaluation Plan below)*
    - Pilot investigators will be asked to provide both informal and formal feedback on both the eLearning module and the gamified assessment.
    - Review feedback provided by trainees submitted through weekly surveys (four per training class). Compile all feedback collected during pilot phase.
    - Review feedback provided by security supervisor both 30 and 60 days post each pilot training class. Compile all feedback collected during pilot phase.
    - Re-evaluate six months post "Go Live" implementation to assess how well the changes have been integrated and success rate.
    - Communicate progress and suggested revisions to leadership.

Evaluation Plan

Pre-implementation:
A small group of tenured investigators will also be asked to test pilot the elearning and assessment for accuracy and effectiveness. They will be asked to provide formative feedback to compare with data collected from test pilot groups. Security leadership will also review the curriculum design to provide feedback on clarity and accuracy prior to implementation.

The eLearning module and gamified assessment will be piloted in several training classes. Both assessments will be comprised of multiple-choice questions and will provide instant feedback on the transfer of knowledge to real-world scenarios. The assessment scores from both evaluations will also be used to measure understanding and effectiveness of the material. In addition to the assessment scores, new investigators will also be asked to provide informal feedback. If they liked the elearning, understanding, clarity, and any other suggestions they have.

New hire investigators will also complete an anonymous survey where they will be asked to provide feedback on both the training and trainer.

All this data will be compiled and analyzed to measure effectiveness and make revisions.

Post Implementation:

Security investigators will complete two assessments to evaluate their understanding of the material. Both assessments will be in the form of a quiz. The eLearning quiz will consist of multiple-choice, true false and fill in the blank questions. The second quiz will consist of multiple-choice questions conducted utilizing gamified simulations. The investigators will be provided with six different call scenarios and will have to answer three to five multiple choice questions for each. They will be provided with immediate feedback upon completion of each assessment. Investigators will be required to pass both assessments with an 80% or higher. They can utilize resources and will have multiple opportunities to complete each assessment until the pass.

Each investigator will be provided with an anonymous weekly training questionnaire to provide feedback regarding the facilitator, as well as the value and understanding of the curriculum. The results will be shared with the instructor to make improvements and adjustments to ensure the learners are motivated and receive adequate training to perform the expected job duties. *See Appendix A for weekly trainee evaluation surveys.*

In addition to assessments completed throughout technical training, investigators will be observed and audited on three calls during their field training. The trainer will audit calls randomly, ensuring that they are selected on three different days. All calls will be graded using the audit rubric that provides a clear and consistent scoring system. *See Appendix C for Call Audit Rubric.* Calls can be audited by live monitoring investigators while they are on the call, or the instructor will listen to call recordings. Live monitoring is the preferred audit method due to the instructor being able to view the investigators screen to audit procedural skills. The system used to record calls doesn't always capture screens. Instructor views the investigator's screen to verify they are using resources, manual chapters, notes, reviewing account activity in the proper systems, taking proper notes, actioning the accounts appropriately, as well as transferring the victim to the appropriate department if applicable. The instructor will provide detailed notes for each call to include the call type, strengths, and areas of opportunity. Investigators calls during training are typically 30-60 minutes long. The instructor can spend anywhere between 2–3.5 hours conducting call audits. Audits will be reviewed by the investigators supervisor to assess progress and identify areas of opportunities that can be monitored and addressed (if needed) post training. Investigators will be provided feedback from audits by the instructor but will not be provided with a copy of the audits conducted. In order to complete training to transition to their job role, investigators are required to pass their call audits with an average of 80% or higher.

(*This assessment method is used in training because it is the monthly assessment used post-training. Investigator's supervisor's audit three calls and provide the investigator feedback. Investigators are expected to review feedback provided to improve performance. This assessment method is being re-evaluated by training due to the amount of time spent per investigator auditing calls).*

Security Leadership will also provide feedback on new investigators performance post-training to evaluate transfer of learning to performance success. This data will be collected using surveys given 30- and 60-day post-training. Leadership's evaluation feedback will be used to identify any additional gaps in curriculum that need to be addressed. *See Appendix B for Security Leadership Evaluations*.

The trainer will also submit a discrepancy report at the end of each training session. The discrepancy report will note any updates or changes that need to be made to keep the curriculum current with systems, procedures, and manual chapters. Discrepancies reported will be corrected prior to the next training session.

Appendix A

Survey: Weekly Survey or One Day Course Training Evaluation

Class and Trainer Information:
Date:
Business Unit:
Class ID:
Trainer(s) Name:

Is this either a ONE DAY COURSE or the FINAL WEEK OF TRAINING?
Indicate the Week of course:

Feedback Questions using 5 point Like-hart scale:
1 – Strong Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4- Agree, 5 - Strongly Agree

Q1: The trainer spent appropriate time reviewing course material:
Q2: The trainer clearly explained difficult topics:
Q3: The trainer encouraged questions and provided clear feedback to aid in my development:
Q4: The trainer demonstrated respect for each learner:
Q5: When necessary, the trainer kept the classroom free of distracting discussions and other interruptions:
Q6: The activities completed will prepare me for future success in my role.:
Q7: The trainer properly prepared me for my role by providing instruction/guidance on how to use my resources to find answers:
Q8: The trainer was knowledgeable of the subject matter:

Open-ended Questions:

Q9: Do you have any unanswered questions from the material covered this week or a topic that you would like the trainer to revisit?

Use the box below to leave any additional comments on the trainer or classroom environment.:

Security Investigator Training Evaluation Final Week:

Class and Trainer Information:
Date:
Business Unit:
Class ID:
Trainer(s) Name:

Feedback Questions using 5 point Like-hart scale:
1 – Strong Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4- Agree, 5 - Strongly Agree

FQ1: I was well engaged with what was going on during training.:
FQ2: I was able to demonstrate what I was learning.:
FQ3: I understood the purpose of the training.:
FQ4: The activities and exercises aided in my learning.:
FQ5: The materials I received in training were easy to comprehend and will aid in my success.:
FQ6: I will be able to immediately use what I learned.:
FQ7: I believe what I learned will help me be more effective in my job.:
FQ8: I am clear how to specifically apply what I learned.:
FQ9: My trainer(s) facilitated my learning well.:
FQ10: I was comfortable with the pace of training.:
FQ11: I was comfortable with the length of training.:
FQ12: The instructor(s) were key to my success in this course.:

Open-ended Questions:

FQ13: What did you like best about the training?
FQ14: What did you like least about the training?
FQ15: Is there anything else you would like to tell us about your experience with this course?

Appendix B

Security Investigator Performance Evaluation by Leadership 30- and 60- days Post Training:

Class and Trainer Information:
Date:
Business Unit:
Class ID:
Trainer(s) Name:
30- or 60-Day Evaluation:

Open-ended Questions:

Q1: Is the trainee currently meeting the terminal objective of the training?
Q2: What performance gaps (lack of knowledge or skills) are you noticing that need to be addressed in training?
Q3: How much additional training is being provided after the new hire training by mentors, supervisors, or other team members?
Q4: What trends are you noticing in coaching sessions that apply to something that could have been addressed further in training?
Q5: What outcome did you wish to see after training? What kinds of outcomes are you seeing today?
Q6: What would make this training a success in your eyes?
Q7: What key metrics should we see improve because of this training?
Q8: Please let us know of any audit data that might help in a redesign of training. We use collated data to identify pain points and opportunities for improvement.

Appendix C

Security Call Audit Rubric

This rubric should be used in conjunction with the Security Operations Center Call Audit Job Aid and the Security Operations Center Quality Assurance Definitions Document.

Trainee:	
Call Date and time:	

Auditing and Scoring Calls

If…	Then…
The Investigator successfully meets all criteria	Give the Investigator 5-10 points by placing an X in the X Column on the audit form. **Note:** See below for point structure and questions.
The Investigator fails to complete any step that is outlined below	Refrain from placing an X on the audit form. Points will not be awarded. In the **Comments** section of the audit form, leave feedback.

X Column	Opening and Identification	Yes
	Trainee: ➢ Did the Investigator properly identify themselves, their department, and Financial Institution?	5 pts
	Member: ➢ Investigator must obtain the customer's first and last name. ➢ Investigator must obtain the last four digits of the member's SSN. ➢ Investigator must obtain the customer's DOB. ➢ Investigator must also obtain the customer's Codeword if present.	5 pts
	Navy Federal Employee: ➢ Investigator must obtain the employees name and EID. ➢ When a branch calls, the Fraud Investigator must ask the Customer Service Representative (CSR) for their name, EID, and access number. They will enter this information into their Call Tracking System. Verify the CSR has accessed the customer's account. If the employee does not show in the account, the Investigator may not assist.	
	Third Party: ➢ Investigator must ensure they are aware of who there are speaking with at all times. ➢ Investigator should never provide account information to anyone besides the account owner and/or the customer's verified AIF.	

X Column	Maintaining Professionalism	Yes
	Avoids Blame: ➢ Did the Investigator place blame on a peer or different business unit?	5 pts
	Took Ownership: ➢ Did the Investigator take ownership of the call?	5 pts
	Maintained Professionalism: ➢ Did the Investigator stay on topic throughout the call, or did they partake in unrelated conversations?	5 pts
	Maintained Composure: ➢ Did the Investigator show a lack of engagement? Did the Investigator show professionalism?	5 pts

X Column	Secured Accounts & Accurate Information	Yes
	Verify Fraud Activity: ➢ Did the Investigator confirm whether or not fraud occurred on the account? ➢ Did the Investigator review the account to determine fraud occurred that the customer may or may not be aware of?	10 pts
	Followed Proper Procedures:	10 pts

	➢ Did the Investigator follow the steps required to resolve the concern? ➢ Did the employee follow the wrong steps? ➢ Did the Investigator remove the alert in error? ➢ Did the Investigator add the alert in error? ➢ Did the Investigator execute the correct action by removing the credits only?	
	<u>Maintain Call Control:</u> ➢ Did the Investigator allow the caller to dominate the conversation? ➢ Did the Investigator allow the call to go off track? ➢ Did the Investigator advise the caller to keep the conversation relevant to the topic/needs of the call?	10 pts
	<u>Ask Accurate Probing Questions and Determined Intent:</u> ➢ Did the Investigator ask questions related to the type of fraud? ➢ Did the Investigator ask questions that would determine intent? ➢ Did the Investigator determine intent when there was an opportunity? ➢ Did the Investigator interpret the information correctly?	10 pts
	<u>Provided Accurate Information:</u> ➢ Did the Investigator provide inaccurate information? Did the Investigator check his/her resources?	10 pts
X Column	**Ending the Call**	**Yes**
	<u>Answered All Questions:</u> ➢ Did the Investigator answer all Security Operations related questions? ➢ Did the Investigator fail to answer all SOC related questions?	5 pts
	<u>Summarized the Call:</u> ➢ Did the Investigator review and provide a synopsis to ensure there was a mutual understanding?	5 pts
	<u>Notated Accounts:</u> ➢ Did the Investigator notate the account? ➢ Did the Investigator notate the account with the appropriate information that will aid their peer in the event of a call back?	5 pts
	<u>Tracked Call:</u> ➢ Did the Investigator obtain the application ID, if applicable? ➢ Did the Investigator properly track what type of call was received? ➢ Did the Investigator obtain the access number?	5 pts
Mentor Feedback from RSA/Cyota Splunk Teach Back		
Comments:		

Appendix D

NEEDS ASSESSMENT

A Needs Assessment is the foundational process that ensures training is grounded in the needs of the organization. It identifies how training can help an organization reach its business and performance goals.

The primary needs assessment is a smaller version, or a "Mini Needs Assessment". The primary value of a Mini Needs Assessment is its short duration. Mini assessments can take a few days or a couple weeks, can focus on an immediate problem, and can get quick results.

Needs Analysis Process Model at a Glance

Process	What's Included	Details	Tools to Use	Desired Results
Pinpoint the Problem (What is the problem?)	• Interview Customer/Upper Management • Uncover Issues • Identify Key Stakeholders	• Schedule an interview with the customer/upper management. • Access and read any documents or reports before the meeting. • Identify standards of performance. • Create a list of interviewees (SMEs, users, team members) or request a list from customer. • Following the meeting, summarize and provide the customer/upper management with written feedback on pertinent conclusions. • Write problem definition statements in bulleted list.	• Activity Planning Checklist • Customer Interview Form	Problem Definition (customer defined only)
Confirm the Problem (What evidence exists of the issue/problem?)	• Interview Stakeholders • Assess the effect of the problem on the organization	• Determine method for information gathering (interviews or focus groups). • Schedule interviews, focus groups, or informational meetings. • Send the questions to interviewees in advance. • Determine how the issue/problem affects the organization/BU/Unit.	• Process Model Checklist • Stakeholder Interview Questions • Focus Group Questions	Findings
Seek Solutions (What is the most viable solution?)	• Consider appropriate solutions • Gain consensus on action plan	• Prioritize solutions. • Ensure the solutions are consistent with the strategic or business goals of the organization. • Categorize the solutions (list of procedures/ tasks/employee position). • Present to customer/ upper management for approval.	• Activity Planning Checklist • Interview Questions	Action Plan

Needs Assessment Activity Planning Checklist

See "Data Gathering Resources Chart" that further identifies the details of collecting information for each item on the checklist.

		Activity	Description	Resource	Team Member(s)
☐	1.	Business Analysis	• Project intake documentation • Identify business goals	Customer	Upper Management/ Project Manager
☐	2.	Conduct Individual Interviews (business related)	• Identify and map key processes for each business goal • Identify key roles and tasks related to each business goal • Identify factors in the work environment that influence the achievement of business goals • Prepare project charter, submit to customer, final goes to ID	Customer, Learner's managers	Upper Management/ Project Manager
☐	3.	Conduct Individual/Group Interviews (as needed)	• Identify and map key processes • Identify key roles and tasks • Identify influences in the work environment • Collect existing data	SMEs, Trainers, High performers	Instructional Designer(s), Documentation Specialist(s)
☐	4.	Conduct Work and Work Product Observations	• Identify and map key processes • Identify key roles and tasks • Identify influences in the work environment	SMEs, Trainers, High performers	Instructional Designer(s), Documentation Specialist(s)
☐	5.	Conduct Surveys (as needed)	• Identify and map key processes • Identify key roles and tasks • Identify influences in the work environment	SMEs, Trainers, High performers	Instructional Designer(s), Documentation Specialist(s)
☐	6.	Design Solutions/ Procedure Solution	• Select solutions that are appropriate to the roles, tasks, and influences and can be designed within the program constraints • Plan a strategy for implementing each solution (include new procedure if required)	NA	Instructional Designer, Documentation Specialist (if new procedures/ manuals are required)
☐	7.	Plan Evaluation	• Identify methods for evaluating the recommended solutions using Kirkpatrick levels	NA	Instructional Designer
☐	8.	Write Analysis Report	• Prepare needs assessment results and recommended solutions for presentation to customer/team members	NA	Instructional Designer(s), Documentation Specialist(s)

Data Gathering Resources

Data collection is vital to the needs assessment. Potential resources can be acquired to aid in the needs assessment process.

Source	Type of Data	Advantage	Disadvantage	Needs Assessment Activity Planning Checklist Item
Extant data: reports, studies, business docs	Business needs	Data collected previously	Not collected specific for needs assessment purpose; extrapolate data to get necessary information	1
Upper management/client	Business needs	Identify priorities and goals of the business	Limited or non-existent as access permitted	1
Learners' managers	Desired performance Current performance	Can speak clearly to the desired results of learners and on-the job behaviors.	My want to dictate the learning result; keep managers on track to only address performance.	2
Subject matter experts (SMEs) or resource materials	Desired performance Desired knowledge and skills	Provide picture of peak performance and knowledge/skills	Expertise may not translate to learning; needs assessor must do that.	2
Extant data: job descriptions, aggregate performance evaluation data	Current performance	Data exists; easy to obtain; client may provide	Not collected specific for needs assessment purpose; extrapolate data to get necessary information	3
Customers	Desired performance Current performance	Provide a clear picture of desired outcome	May not consider logistics, time, and expense	3, 4, and 5
Learners	Current performance Learning needs Learner needs	State what they do now, what they needs to learn, how they need to learn	May not be comfortable sharing all information	3, 4, and 5
Other training professionals	Learning needs Learner needs	If they have trained the content in the past, can provide what worked and didn't work. May assist as SME.	Can be biased to their own training methods	3, 4, and 5
Extant data: previous training evaluation information	Learning needs Learner needs	Provides learner's perceptions and what works for them in the learning environment	May have not thoroughly evaluated and provided complete information	3, 4, and 5
High performers	Desired performance	Display excellent performance and serve as the model for peak performance	Performance second nature and can't identify components; needs assessor must do that	3, 4, and 5

NEEDS ASSESSMENT CUSTOMER/UPPER MANAGEMENT INTERVIEW GUIDE

Name/Position: _____

Date: _____

Purpose: To obtain Customer/Upper Management perspective of a performance problem.

Instructions: Rate each of the following items. The scale is as follows: 1 = very poor, 2 = poop, 3 = average, 4 = high, 5 = very high. If an item is not applicable, mark NA. Space has been provided for additional notes.

Note: Training is not always the recommended solution for every performance problem. Only problems for which training is considered an appropriate solution are stated with "provide training".

Problem Indicator	Poor				High	Possible Solution
A. Knowledge or skill problem?						
1. Knowledge of job-related responsibilities.	1	2	3	4	5	Will job aids help? If not, provide training.
2. Proficiency in technical skills needed to perform job or tasks.	1	2	3	4	5	Provide training.
B. Job performance problem?						
1. Availability of documents such as job aids, reference guides, or manuals.	1	2	3	4	5	Increase number.
2. Knowledge of how performance will be measured.	1	2	3	4	5	Provide information or conduct briefing.
C. Existing training problem?						
1. Quality of prerequisite training.	1	2	3	4	5	Provide training.
2. Quality of training personnel.	1	2	3	4	5	Provide train-the-trainer training.
3. Quality of training material.	1	2	3	4	5	Audit and revise materials.
D. Environmental problem?						
1. Accessibility to internal customers.	1	2	3	4	5	Improve communication channels.
2. Availability of internal customers.	1	2	3	4	5	Improve work flows.

Problem Indicator	Poor				High	Possible Solution
E. Attitude problem?						
1. Value of job/tasks.	1	2	3	4	5	Increase job responsibilities.
2. Opportunity for feedback on performance from peers.	1	2	3	4	5	Build periodic assessment and feedback schedule between manager and individuals or groups.
3. Opportunity for feedback on performance from managers.	1	2	3	4	5	Same as above.
F. Motivation problem?						
1. Ability of group to meet unit goals?	1	2	3	4	5	Evaluate unit goals. Provide rewards.
2. Tolerance for mistakes by management.	1	2	3	4	5	Change organizational culture
3. Quality of cooperation between units.	1	2	3	4	5	Promote cooperation through inter- or intragroup activities.
G. Compensation/incentives problem?						
1. Value for compensation scales.	1	2	3	4	5	Increase pay scales.
2. Value for incentive structures.	1	2	3	4	5	Change incentive structures.
3. Knowledge about incentive/reward structures.	1	2	3	4	5	Provide information.

When the customer/upper management/other stakeholders have identified "*B. 1. Job Performance; availability of documents/manuals*" then the Documentation Specialist will complete a Needs Assessment regarding documentation that will need to be created. See "Interview Questions for Manual/Procedure Development Guide".

INTERVIEW QUESTIONS CUSTOMER/UPPER MANAGEMENT GUIDE

Name/Position: _____

Date: _____

Deadline requested date: _____

BUSINESS NEEDS

1. What are the business issues/problems?	2. What is causing the problems?
3. Can any external factors be causing the problems?	4. When did the problems first occur?
5. When do the problems typically occur?	6. What has been done to resolve the problem?

PERFORMANCE NEEDS

7. What are the standards for performance? Can you provide those in a written format?	8. Which stakeholders/team members are affected by the problems?
9. How are the stakeholders/team members affected by the problems?	10. Are other units or departments being affected by the problems? Please name them.

11. How is the organization as a whole being affected by problems?	12. What other additional information can you provide?

LEARNING NEEDS

13. What knowledge and skills do targeted employees need to learn to perform the way they should?	14. What is the level of performance required (percentage)?
15. What availability will the learners have for training (time available)?	16. What are their learning styles?
17. How is the organization as a whole being affected by problems?	18. What other additional information can you provide?

INTERVIEW QUESTIONS FOR MANUAL/PROCEDURE DEVELOPMENT GUIDE

19. What are the key processes? Provide list if possible.	20. What existing documentation/material can you provide?
21. What roles and personnel are included?	22. What is the availability for work observations? Schedule for daily, weekly meetings?
23. Are there specific regulations that should be included or effected?	24. What is the level of complexity for each of the key processes? Highly detailed, moderate, simple. State for each of the key processes identified.
25. What modality will be used to share with the users? LAN, SharePoint, eNet, other?	26. What systems are used to complete the key processes? Can access be provided to SMDLS?
27. Who are the reviewers and final approvers?	28. What is the preferred method for document reviews? For example, email, SharePoint, in-person
29. What is the communication plan for the new procedures?	30. Who are the analysts/testers involved in the new system implementation? What is their availability for this project?