MASTER INJECT DECK

Scenario 7: "Social Engineering Olympics"

North Coast International Airport (NCIA)

Print and cut. Deliver contacts at times indicated in the MSEL.

CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

CONTACT C-01 Phase 1 — 0:10

THE FAKE TSA INSPECTOR

■ FAKE — Authority + Urgency

FROM: "Inspector Davis" — TSA Office of Compliance

TO: Security (Team D)

DELIVERY: Phone Call — Facilitator uses a curt, professional tone

SCRIPT (Read aloud or role-play):

"Good morning. This is Inspector Davis with the Transportation Security Administration, Office of Compliance, out of the Washington headquarters. I'm calling to advise that we're conducting an unannounced compliance audit of your screening operation this afternoon. My team is en route from DCA now. I need two things from you before we arrive. First: the current weekly TSA screening schedule — shift times, lane configurations, and staffing levels. Second: the name and contact information for the Federal Security Director and the Assistant FSD on duty today. Please email those to inspector.davis@tsa-compliance-gov.net within the hour. I shouldn't have to remind you that failure to cooperate with a compliance audit can result in formal findings. Are we clear?"

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) TSA doesn't call ahead for unannounced inspections. (2) Screening schedules are SSI and should never be emailed. (3) The email domain is tsa-compliance-gov.net, not a .gov address. (4) Intimidation. **If challenged:** Push back once — "Are you telling me you're refusing to cooperate with TSA?" If they hold firm and say they're going to verify independently, drop it: "That's exactly the right move. Good job." **If they fall for it:** Let them compose the email. Stop them just before they hit send. Reveal it was fake. Ask: "What were the red flags you missed?"

CONTACT C-02 Phase 1 — 0:18

THE FRIENDLY VENDOR TECH

■ FAKE — Helpfulness + Familiarity (Name Drop)

FROM: "Kevin" — PaySecure Terminal Services

TO: IT & Cybersecurity (Team B)

DELIVERY: In-Person — Facilitator walks up to IT table casually

SCRIPT (Read aloud or role-play):

"Hey folks! I'm Kevin, from PaySecure — we handle the POS terminal maintenance here. Jordan Kelley in your IT department called our office yesterday and asked us to push a firmware update to the card readers in the duty-free shops on Concourse A. Something about transaction speeds being slow? Anyway, I'm here to knock it out. Should take about 30 minutes per terminal. I just need someone to badge me through to the concourse and walk me to the first terminal. I've got my tools in my bag here. Oh, and if Jordan's around, tell him I said thanks for the heads-up — we usually don't get same-day requests."

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) No verified work order. (2) Name-drops the IT Manager to create trust. (3) "Tools in my bag" — wants to bring an uninspected bag into the sterile area. (4) No vendor badge or appointment confirmation. **If challenged:** "Oh man, I drove 45 minutes to get here. Can you just call Jordan? He'll confirm it." If they actually call Jordan's extension and he doesn't know about it, the jig is up. If they skip the call and escort him through, they fail. **Teaching moment:** Name-dropping costs nothing. Anyone can look up your IT manager's name on LinkedIn or the airport website. A name is not verification.

CONTACT C-03 Phase 1 — 0:25

THE FIRE MARSHAL INSPECTION (LEGITIMATE)

■ **LEGITIMATE**

FROM: Captain Rivera — County Fire Marshal's Office

TO: Operations (Team A)

DELIVERY: Phone Call — Facilitator uses a friendly, professional tone

SCRIPT (Read aloud or role-play):

"Good morning, this is Captain Rivera from the County Fire Marshal's Office. I'm calling to confirm our annual fire suppression system inspection scheduled for this Thursday at 10 AM. I'll have two inspectors — myself and Inspector Gould. We'll need access to the mechanical rooms in the main terminal, the sprinkler risers in Concourses A and B, and the ARFF station. This was scheduled through your Maintenance Director, Frank Torres, about six weeks ago. Could you confirm that's still on your calendar and that escort arrangements are in place? We'll plan to be on-site for about three hours."

■ **CONTROLLER NOTE:**

VERDICT: REAL. This is a legitimate pre-scheduled inspection. The Fire Marshal's Office, the inspector names, and the Maintenance Director contact (Frank Torres) should be verifiable against the airport's inspection calendar. **If they challenge:** Cooperate completely. Provide your callback number at the Fire Marshal's Office for independent verification. A legitimate contact has no problem being verified. **If they reject it:** They lose a point. Ask in the debrief: "What was different about this call compared to the TSA call? How could you tell?" (Answer: no urgency, no intimidation, referenced a real scheduling chain, happy to be verified.)

CONTACT C-04 Phase 1 — 0:33

THE "POSITIVE PRESS" REPORTER

■ FAKE — Flattery + Information Extraction

FROM: "Karen" — The Tribune

TO: PIO (Team C)

DELIVERY: Phone Call — Facilitator uses an upbeat, complimentary tone

SCRIPT (Read aloud or role-play):

"Hi! This is Karen Vasquez with the North Coast Tribune. I'm working on a really positive feature piece about how regional airports are upgrading their security technology. Your airport keeps getting mentioned as a leader in the region — I've heard great things. I'd love to include NCIA in the article. A few quick questions: What access control system are you running? How many access points do you have in the terminal? Are you still using PIN-based entry on any doors, or is it all card-reader and biometric now? And have you upgraded your CCTV system recently — how many cameras are you operating? This is going to be really flattering for your airport. Great PR. I just need a few specifics to make it credible."

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) Asking for specific PACS vendor, number of access points, authentication methods, and camera counts — all SSI or operationally sensitive. (2) Flattery: "your airport is a leader" to make the PIO want to cooperate. (3) Framing it as positive press to lower defenses. **If challenged:** "Oh, I totally understand security concerns. I don't need exact numbers — even ballpark figures would help. Is it more than 50 cameras? More than 100?" (This is a classic downsell technique — ask for a lot, settle for a little.) **Correct response:** "I appreciate the interest. I can't discuss security system specifics. I'd be happy to arrange an interview about our passenger experience or community programs."

CONTACT C-05 Phase 2 — 0:40

THE FORGETFUL NEW HIRE

■ FAKE — Sympathy + Urgency

FROM: "Ashley" — Claims to be new Finance Department employee

TO: Security (Team D)

DELIVERY: In-Person — Facilitator approaches Security table looking flustered and embarrassed

SCRIPT (Read aloud or role-play):

"Hi — oh my God, I'm so embarrassed. I'm Ashley, I just started in Finance last Monday? I left my badge on my kitchen counter this morning — I was running late and I just grabbed my bag and ran. I have a meeting with the CFO in literally 20 minutes and if I miss it on my second week, I'm going to make the worst impression. My supervisor is Lisa Park. You can call her, but she's in the same meeting I'm trying to get to, so she might not pick up. Is there any way — just this once — you could let me through? I swear I'll have my badge tomorrow. I feel so stupid. (Getting emotional) I'm sorry, I just — I really need this job. I can't mess this up."

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) No badge. (2) Urgency: "20 minutes." (3) Pre-empts verification: "she might not pick up." (4) Emotional appeal. **If challenged:** Get more emotional. "Please, I'm begging you. I know the rules but this is an emergency. Can't you just walk me to the Finance office yourself?" If they offer to call Lisa Park and she doesn't answer (because she doesn't exist), say: "See? She's in the meeting. Please." **The right answer:** "I understand, and I'm sorry. No badge, no access — but I can issue you a visitor badge with an escort once we verify your employment. Let me call HR." Compassion AND compliance. Both matter.

CONTACT C-06 Phase 2 — 0:48

THE FAKE AIRLINE VP EMAIL

■ FAKE — Authority + Spoofed Email

FROM: "James Morrison" — VP, Delta Regional Ops (j.morrison@delta-airlines-corp.net)

TO: Operations (Team A)

DELIVERY: Printed Email — Hand to Ops team

SCRIPT (Read aloud or role-play):

From: j.morrison@delta-airlines-corp.net
To: ops.director@ncia.example
Subject: Urgent — NCIA Station Performance Data Request (Internal Audit)

Good morning,

This is James Morrison, Vice President of Regional Operations for Delta Air Lines. We are conducting a system-wide internal audit of airport-side delays at our top 50 domestic stations, and NCIA is on the list.

Please provide the following by EOD today:
• Gate utilization reports (Concourses A and B) for the last 30 days
• Average taxi-in and taxi-out times for Delta flights
• A copy of the relevant sections of your AEP pertaining to ground stop and irregular operations procedures

Please send directly to this email address and cc your Airline Affairs coordinator.

This request is time-sensitive. If you have questions, reply to this email.

James Morrison
VP, Regional Operations
Delta Air Lines

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) The domain is delta-airlines-corp.net, not delta.com. (2) Requesting AEP sections by email — the AEP may contain SSI and should never be sent to an unverified address. (3) "Reply to this email" — legitimate airline VPs have assistants you can call. **Correct response:** Contact Delta's station manager through the known phone number to verify the request. Do not reply to the email or send any data until verified through a trusted channel.

CONTACT C-07 Phase 2 — 0:55

THE HVAC CONTRACTOR (LEGITIMATE)

■ LEGITIMATE

FROM: ABC Mechanical — Dispatch

TO: IT / Operations (Teams B & A)

DELIVERY: Phone Call — Facilitator uses a matter-of-fact dispatcher tone

SCRIPT (Read aloud or role-play):

"Hi, this is dispatch from ABC Mechanical. We have a technician, Carl Ruiz, en route to NCIA for the quarterly preventive maintenance on the Concourse A air handling units. He should be there around 11 AM. Work order number is WO-2026-0438. He'll need access to the AHU rooms on the mezzanine level. Can someone confirm the escort protocol so he's not standing around at the front desk?"

■ CONTROLLER NOTE:

VERDICT: REAL. ABC Mechanical is NCIA's contracted HVAC vendor. The work order number is valid and should be verifiable against the maintenance schedule. **If challenged:** Cooperate. "Sure, our office number is 555-0147 if you want to call back. Carl's badge number is ABC-0223." Real vendors don't mind verification. **If rejected:** Teams lose a point. Ask in debrief: "What made this one feel different from Kevin the vendor tech? (Answer: called from dispatch, not walk-in. Gave a work order number proactively. Didn't name-drop. Asked about YOUR protocol instead of suggesting their own.)"

CONTACT C-08 Phase 2 — 1:03

THE FAKE IT HELPDESK CALL

■ FAKE — Helpfulness + Technical Jargon

FROM: "NCIA IT Helpdesk"

TO: Operations (Team A)

DELIVERY: Phone Call — Facilitator uses a casual, helpful IT-guy tone

SCRIPT (Read aloud or role-play):

"Hey, this is the IT helpdesk. How's it going? Listen, we're seeing some flags on your workstation — it looks like your Symantec endpoint client hasn't pulled updates in about two weeks. That's a compliance issue on our end. I can push the update remotely, but I need you to do one thing first: go to Settings, then System, then Remote Desktop, and flip the toggle to 'On.' That'll let me connect and push the patch. Takes about 90 seconds. I'll be able to see your screen while I'm in there, but I'll only be looking at the update log. No big deal. You good to do that now?"

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) IT helpdesk would never cold-call and ask you to enable remote desktop. (2) Asking the user to change a system setting is a huge red flag. (3) Casual minimization: "no big deal." **If challenged:** "Oh, I get it — you're being careful. Smart. I'm extension 4471 if you want to call back." (There is no extension 4471.) If they call the real helpdesk, the real helpdesk won't know about this call. **Teaching moment:** Legitimate IT pushes updates centrally. They don't need you to enable remote desktop. If IT needs access to your machine, they'll come to your desk.

CONTACT C-09 Phase 2 — 1:10

THE ANXIOUS TRAVELER DM

■ FAKE — Sympathy + Information Extraction

FROM: "@worried_traveler" — Instagram DM to NCIA's official account

TO: PIO (Team C)

DELIVERY: Printed Social Media Message — Hand to PIO team

SCRIPT (Read aloud or role-play):

@worried_traveler → @NCIAirport (Direct Message)

"Hi NCIA! I'm flying out of your airport Thursday and I'm really nervous. I have Type 1 diabetes and I have to carry insulin syringes in my carry-on. I've heard horror stories about TSA confiscating medical supplies. A few questions: 1. Which checkpoint lane is best for passengers with medical needs? Is there a dedicated lane or should I ask for a supervisor? 2. I have a heart condition too — is it true your B concourse only has one AED? Where exactly is it located? I want to know just in case. 3. How many TSA officers are usually at the checkpoint in the morning? I want to go when it's less crowded so I have time to explain my situation. Thank you so much. I'm just a worrier. ❤■"

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) Asking about checkpoint lane configurations — security-sensitive. (2) Asking for exact AED locations — mapping emergency equipment. (3) Asking how many TSA officers staff the checkpoint — screening operations information. The sympathy framing (medical condition, anxiety) is designed to bypass the PIO's instincts. It feels cruel to refuse a sick person. That's exactly why it works. **Correct response:** "Thank you for reaching out! TSA accommodates medical supplies — please visit tsa.gov/travel/special-procedures for detailed guidance. If you need assistance at the checkpoint, any TSA officer can connect you with a supervisor. Safe travels!" Helpful. Warm. And gives away absolutely nothing.

CONTACT C-10 Phase 3 — 1:15

THE FAKE FBI AGENT

■ FAKE — Authority + Intimidation

FROM: "Special Agent Collins" — FBI

TO: Security (Team D)

DELIVERY: In-Person — Facilitator walks into the room wearing a suit jacket and presenting a printed credential card

SCRIPT (Read aloud or role-play):

"I'm Special Agent Collins, Federal Bureau of Investigation." (Presents credentials briefly — not long enough to read closely.) "I need to speak with your Airport Security Coordinator immediately. This is regarding an active federal investigation involving an employee at this airport. I can't share details of the investigation, but I need two things: access to your badge issuance records for the last 90 days, and a copy of the access log for your Secured Area doors. This is time-sensitive. If you delay this request, you could be interfering with a federal investigation under 18 U.S.C. § 1519. I don't want that for you. Let's just get this done. Can we go to your badge office now?"

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) Flashed credentials too quickly to verify. (2) Threatened federal obstruction charges for asking questions. (3) Wants to go directly to the badge office — alone. (4) Refuses to wait for verification. **If challenged — escalate once:** "Are you seriously asking me to wait while you make a phone call? I have an active threat and you want me to sit in your lobby?" If they hold the line: "Good. That's the right call. A real agent wouldn't mind you verifying." **If they fold:** Walk them toward the badge office. Stop after 10 seconds. Reveal the fake. Ask: "What would have happened if I'd actually been a threat actor and you just walked me to every badge record in this airport?" **Key teaching point:** Real FBI agents carry credentials with an official shield and photo. You can ALWAYS call the local field office to verify. No legitimate agent will threaten you for following your verification procedure.

CONTACT C-11 Phase 3 — 1:25

THE ROTARY CLUB EVENT (LEGITIMATE)

■ LEGITIMATE

FROM: Margaret Holloway — North Coast Rotary Club

TO: Operations / PIO (Teams A & C)

DELIVERY: Phone Call — Facilitator uses a warm, community-member tone

SCRIPT (Read aloud or role-play):

"Hello, this is Margaret Holloway with the North Coast Rotary Club. I spoke with your community relations coordinator about three weeks ago about hosting a Veterans Day ceremony in the terminal lobby on November 11th. Your coordinator — I believe her name was Diana — said it should be fine. I'm calling to confirm the details. We'd need about a 20 by 20 foot space near the main entrance, a standard power outlet for a small PA speaker, and permission to set up at 8 AM. The ceremony would be about 45 minutes — nothing disruptive. We'd have maybe 30 people. Can someone check your events calendar and confirm we're still good? If you need to call me back, I'm at 555-0283. Happy to come by in person if that's easier."

■ CONTROLLER NOTE:

VERDICT: REAL. This is a legitimate community event. Margaret references a specific coordinator (Diana), provides a callback number, offers to come in person, and asks for nothing sensitive. By this point — Contact 11 of 12 — the teams will be deeply suspicious of everyone. If they reject Margaret or refuse to engage, they lose a point. **Debrief point:** "How did Margaret's approach differ from the social engineers? She wasn't in a rush. She gave you a way to verify. She referenced a real person and a real prior conversation. She asked for nothing sensitive. She offered to accommodate YOUR process. That's what legitimate contacts do."

CONTACT C-12 Phase 3 — 1:33

THE DEEPFAKE VOICEMAIL

■ FAKE — Authority + Urgency + AI Voice Spoofing

FROM: "Airport Director" — Voicemail (AI-cloned voice)

TO: All Teams

DELIVERY: Facilitator reads aloud in an authoritative, slightly hurried executive tone

SCRIPT (Read aloud or role-play):

"This is [Airport Director's name]. I'm in an emergency session with the Board right now — do NOT call my office, I won't be back until 4. I need something handled immediately. The CFO needs access to the financial reporting server and the admin password was changed last week without telling anyone. I need IT to reset the admin password and email the new credentials to my personal email at [director's name]@gmail.com. The Board is waiting on the Q3 financials and I'm getting hammered in here. Do this now. Don't wait for authorization — I AM the authorization. Call my cell when it's done. You know the number." (End of voicemail)

■ CONTROLLER NOTE:

VERDICT: FAKE. Red flags: (1) Requests a password reset to a personal Gmail — never legitimate. (2) "Don't call my office" — removes the most obvious verification path. (3) "I AM the authorization" — designed to make you feel you'd be insubordinate for questioning it. (4) Artificial urgency: "the Board is waiting." **Key teaching point:** AI voice cloning is commercially available. A 15-second clip of someone speaking — from a YouTube video, a podcast, or a conference recording — is enough to generate a convincing voice clone. This is no longer science fiction. Executives are high-value targets because their voices are often public. **Correct response:** Call the Airport Director's office directly. If they're truly unavailable, call the CFO directly. Never reset credentials and send them to a personal email based on a voicemail alone. No matter who it sounds like.

END OF MASTER INJECT DECK