FACILITATOR GUIDE, MODULE 01: ACCOUNT TAKEOVER AND SYNTHETIC IDENTITY

# How to teach the one about *the code*

Everything a volunteer needs to deliver this module competently: what to do in the twenty minutes before, how to run each segment, what the exercise is actually testing, what to do when somebody says it happened to them, and what never to do regardless of how much it would help.

THE SHAPE OF THIS SESSION — 45 MINUTES · FOUR FIXED PARTS

**0:00 to 0:14**

PART 01

### How the schemes work

Two tracks, kept visibly separate. A takeover that runs in an hour, and an identity built over years.

**0:14 to 0:21**

PART 02

### The specific signals

Set A during a takeover, Set B in the mail. Spend the time on Set B.

**0:32 to 0:38**

PART 03

### The single action

A code you did not ask for is not a code to give. Plus the one setting: the freeze.

**0:38 to 0:43**

PART 04

### Where to report

IdentityTheft.gov said out loud, and the three bureau numbers on the handout.

**The exercise sits between parts 02 and 03, from 0:21 to 0:32.** It is the longest single block in the session and the first thing a nervous facilitator cuts. Do not cut it. Everything before it is explanation, and explanation on its own has never changed what anybody does on a Tuesday afternoon.

| | | |
|---|---|---|
| COVERS<br>**Module 01 only**<br>Each module has its own guide | TEACH IT TO<br>**Anyone with a bank account**<br>Effectively everyone. Good first session. | PREPARATION<br>**90 minutes, first time**<br>20 minutes each delivery after |
| SESSION LENGTH<br>**45 minutes**<br>30 minute cut included | THE MODULE<br>**[LINK]**<br>Read it before this guide | VERSION<br>**[VERSION]**<br>Published [DATE] |

| | |
|---|---|
| LICENSE<br>**CC BY 4.0**<br>Copy, adapt, and teach it | GOVERNING RULES<br>**Your host organisation's**<br>Where they differ from this, theirs win |

## What this guide is

### Written so that the author is not required

Material that only works when its author is in the room is a service. Material a stranger can pick up and deliver well is something else. This guide exists to make the second thing true of Module 01.

The module is derived from fraud detection work: it takes an operational description of how these schemes are built and turns it around into what they look like from the inside. That derivation gives the material its specificity. It does not, on its own, make the material teachable, which is a separate problem with a separate answer.

That answer is the fixed structure shown above. Every module in this series answers the same four questions in the same order, so a facilitator who has run one session knows where everything is in the next. The content is new each time. The floor under your feet is not.

Two things follow, and both are worth saying to anyone about to deliver this. You do not need to be an expert in the schemes. You need to run the shape and be honest about the edges of what you know. And the genuinely difficult part of this session is not technical, it is the thirty seconds after somebody says this happened to me, which is why that section of this guide is the longest.

> **WHERE THIS GUIDE DOES NOT GOVERN**
>
> If you are delivering under the auspices of an organisation, that organisation's conduct rules, safeguarding policy, and escalation procedure take precedence over everything

> written here, without exception. Read theirs first. This guide is written to sit underneath such policies, not to substitute for one.

**This module in particular**

## Four things that make this one harder than it looks

Read these before your first delivery. Each one is a place where a well intentioned facilitator reliably goes wrong, and each has a specific fix.

### It is two schemes, not one

THE STRUCTURAL PROBLEM

Account takeover and synthetic identity get taught together because they both involve identity, and then participants defend against the wrong one. The takeover is fast, loud, and about an account they already have. The synthetic identity is slow, silent, and about a number rather than an account.

**The fix:** keep them physically separate on the board and never let a sentence float between them. Say "that was Track A, now Track B" out loud, more often than feels necessary.

### The most important fact is a negative

THE TEACHING PROBLEM

Synthetic identity accounts carry a different name and a different birth date, so they do not appear on the participant's credit report. This is the single most valuable minute in the session, and it is hard to land because you are asking people to accept that a habit they were previously told was protective is not.

**The fix:** say it, then say why it is not their fault, then give them the thing that does work, which is the freeze. Never leave the negative sitting on its own.

### Shame runs higher here than in the other modules

THE ROOM PROBLEM

In the Medicare module, victims failed to notice something. In this one they handed something over, usually while being polite to someone on the phone. That difference is felt keenly and it keeps people quiet.

**The fix:** name the design early and to the whole room, not to any individual. These operations are staffed, scripted, and rehearsed against thousands of people, and the script is built to work on careful people.

---

### Somebody in the room may be mid incident

THE URGENCY PROBLEM

Unlike the other modules, this one describes things that happen in an hour. A participant may realise during your session that their phone lost service this morning, and that is a live emergency rather than a story about last year.

**The fix:** know the first branch of the disclosure path before you start, and be willing to interrupt your own session for it.

---

First delivery

## Before you teach this one for the first time

About ninety minutes, once. Everything after this is the twenty minute routine in the next section.

Step 1

### Read the module end to end

Including its facilitator notes, which are the part people skip. Do not jump to the run sheet. The reasoning behind the wording is what lets you answer a question the module did not anticipate.

Step 2

### Do the credit file exercise cold

Before reading the answers. You will probably flag the store card, and that experience is what stops you dismissing a participant who does the same.

Step 3

### Say the two specimen messages aloud

The bank's code message, then the caller's, ninety seconds apart. Hearing yourself deliver that pair for the first time should not happen in front of thirty people.

Step 4

### Freeze your own credit first

All three bureaus, before you tell a room to do it. You will then be able to say how long it took and what the website asked for, which is worth more than the instruction itself.

**The five sentences to be able to say without notes**

If you can say these without looking down, you can run the session even when the projector fails and the printouts did not arrive.

- [ ] "A code you did not ask for is not a code to give. It is a notice that somebody is already trying to get in."
- [ ] "Freeze your credit at all three bureaus. It is free by law, it does not affect your score, and lifting it takes minutes."

- [ ] "These accounts do not show up on your credit report, because they are in somebody else's name. There is nothing there to see."
- [ ] "These operations are staffed, scripted, and rehearsed against thousands of people. Being taken in by one is not a failure of intelligence."
- [ ] "I do not know, and here is who does."

---

Every delivery

### The twenty minutes before

Short, and not optional. Two of these are the items that actually go wrong: out of date bureau numbers, and a facilitator who has not read their own organisation's escalation procedure.

- [ ] **Verify the three credit bureau numbers and the FTC number.** These change more often than the federal helplines do, and a number read confidently from a slide and answered by nobody undoes the session.
- [ ] **Check that the credit freeze is still free by federal law** and that nothing has changed about how it is requested. This is the load bearing fact of the whole session.
- [ ] **Read your organisation's escalation procedure,** specifically for suspected coercion, cognitive decline, or financial exploitation by a family member.
- [ ] **Print the handout at 14 point or larger,** and bring the credit file exercise as a separate sheet. Bring more than you think you need.
- [ ] **Bring a pen and paper for yourself.** You will need to write down a question you cannot answer, in front of the person who asked it. Doing that visibly is part of the answer.
- [ ] **Check the room.** Can everyone hear you from the back with the door open? Is there glare on the screen? Fix it now, not at minute ten.

- [ ] **Decide who takes a disclosure** if you are co facilitating, so one of you can step out with somebody without the session stopping. This module needs that more than the others.

- [ ] **Put your own phone away.** A facilitator checking a screen during a session about not trusting screens is a worse look than it sounds.

> **IF YOU ARE DELIVERING VIRTUALLY**
>
> Say at the very start that nobody should type an account number, a verification code, or a Social Security number into the chat, because in a virtual room somebody eventually will. Put every phone number in the chat as well as saying it, expect that some participants cannot see the chat, and say each number slowly twice regardless. Send the handout in advance rather than after.

---

Segment by segment

## Running the forty five minutes

The module carries the run sheet. This is the annotated version: what to say, what to watch for, and where facilitators reliably lose time.

| 0:00 to 0:04<br>OPEN | **Read the two messages, then ask the wrong question on purpose**<br>Read the bank's code message. Then the caller's, ninety seconds later. Then ask: "Which one of these is fake?"<br>Most rooms say the first one. The answer that lands is that the first is entirely real, the bank did send it, and that is precisely why the second one worked.<br>**WATCH FOR**<br>Do not announce the topic before reading the messages. Starting with "today we are talking about identity theft" gives everybody permission to decide it does not apply to them. |
|---|---|

0:04 to 0:14

PART 01

### The two tracks, kept apart

Walk Track A across four steps, then Track B across four steps. Write "A" and "B" on the board and point at which one you are in.

The minute that matters is inside Track B. Say plainly that the fake person's accounts carry a different name and never appear on the participant's own credit report.

> *"You can check your credit report every month for ten years and never see this one. There's nothing there to see. That's not a failure on your part, it's how the scheme is built."*

**WHERE THE TIME GOES**

This is the segment that runs long. If you are over at 0:15, cut variants rather than compressing Track B, because Track B is the part nobody else has told them.

0:14 to 0:21

PART 02

### The signals, quickly then slowly

Read three of the quoted caller lines aloud, in the caller's voice rather than off the page. Ask who has heard something close to one of them. Hands go up, and that is the moment the room engages.

Cover Set A briskly. Slow down for Set B, because those signals arrive as ordinary mail and get thrown away.

**WATCH FOR**

This is where an unplanned disclosure usually happens. Have the second branch of the disclosure path ready and move on within about thirty seconds.

0:21 to 0:32

EXERCISE

### The credit file, in pairs then together

Hand out the specimen. Four minutes to circle anything they would ask about, alone or in pairs. Then take answers from the room and write every flagged line on the board, including the wrong ones. Reveal only after that.

The full walkthrough of what each line is testing is in the next section of this guide.

> **DO NOT REVEAL EARLY**
>
> Revealing before collecting answers turns the exercise into a lecture and the room stops participating for the rest of the session.

0:32 to 0:38

PART 03

### The action, then the setting

State the single action once, plainly, then have the room say it back to you. Then walk the freeze: three bureaus, free, lifted in minutes, no effect on the score.

> *"A code you didn't ask for isn't a code to give. It's a notice that somebody is already trying to get in."*

> **CORRECT TWO BELIEFS HERE**
>
> That a freeze costs money or hurts a credit score, and that a freeze and a lock are the same thing. A lock is a product some bureaus sell. Nobody needs to buy anything today.

0:38 to 0:43

PART 04

### One number, said out loud

Point at IdentityTheft.gov and the number beside it, and describe what it produces: a recovery plan written for their situation and the sworn report that banks and bureaus ask for.

The handout carries the other eight contacts. One number said aloud beats nine printed.

**0:43 to 0:45**

CLOSE

### Close on the freeze, then stay

Close on the freeze being free and reversible, because it is the one thing they can do this afternoon. Then say you will stay for ten minutes, and stay.

> **THE MOST IMPORTANT TEN MINUTES**
>
> Most disclosures come after the close, not during. Leaving promptly costs the session its most important conversations.

> **THE 30 MINUTE CUT**
>
> Drop the variant list to three (the fraud department call, the phone number takeover, the unrequested new card), cut Set A to the first three signals, and run the exercise for six minutes instead of eleven. **Do not cut the exercise, the freeze, or the reporting segment.** A session that explains the problem and stops leaves people worried and unequipped.

---

**The exercise**

## What each line in the credit file is testing

Seven entries. Three should not be there. The other four are there to teach that unfamiliar is not the same as fraudulent, which is the actual skill.

ANSWER KEY AND TEACHING PURPOSE

| ENTRY | VERDICT | WHAT IT IS TEACHING |
|---|---|---|
| **First Meridian Bank card, opened 2009** | **Fine** | A baseline. Participants need at least one obviously ordinary line so the exercise is a discrimination task rather than a hunt. |
| **Comenity Capital Bank / Garden House store card** | **Fine, and unfamiliar** | The most useful line in the set. Store cards are issued by banks whose names never appear in the shop. Somebody flagging this is behaving correctly, and the answer is "good |

| ENTRY | VERDICT | WHAT IT IS TEACHING |
|---|---|---|
| | | catch, and here is how you would check", never "no". |
| **Harborline Lending Group, line of credit** | **Ask about it** | An open account she did not create, near its limit within four months. The clearest case. Dispute with the bureau, sworn report at IdentityTheft.gov, freeze the same day. |
| **Lakeside Federal Credit Union auto loan, closed 2021** | **Fine** | Closed accounts stay on file for years. Participants often think a settled loan appearing is an error. It is not, and in good standing it is helping them. |
| **Pinegate Auto Finance, hard inquiry** | **Ask about it** | Inquiries precede accounts. Point out that this one is dated weeks before the Harborline account opened, which is what an attempt followed by a success looks like in sequence. Almost nobody reads this section. |
| **Address on file she never lived at** | **Ask about it** | How somebody else receives mail issued in her name. Teach it immediately before the next line so the room learns the distinction rather than the rule. |
| **Name variations: Ruth Ann Whitfield, R A Whitfield** | **Fine** | Bureaus keep every version lenders have reported. Variations of her own name are normal. A name that is not a version of hers at all is the synthetic identity signal, and the pair only teaches that if you run them together. |

**HOW YOU KNOW IT WORKED**

Somebody flags the store card or the closed loan, and leaves understanding both that their instinct was reasonable and that the answer was a phone call rather than a judgment. A room that flags only the three fraudulent lines has learned an answer key. A room that flags five and then sorts them has learned the skill.

The hard part

## When somebody says it happened to them

In a group of thirty older adults, assume at least one. Reread this before every delivery. It is the part where an ordinary session can do real harm, and a good one can do more good than the other forty minutes combined.

START HERE

Somebody indicates, out loud or quietly, that this has happened to them.

IF

### It is happening right now

Money left this week, the phone lost service this morning, a caller is still calling. More likely in this module than in any other.

1. **Treat it as urgent and act during the session, not after.** Speed changes the outcome here in ways it does not for older incidents.
2. Step outside with them, or hand to your co facilitator so the session continues.
3. Have them call their own bank on the number on their card, or their mobile carrier if the phone has lost service. **They dial, they speak.** You stand next to them.
4. Write down for them the time of the call and the name of the person they spoke to. Give them the paper.
5. Return to the room. Do not report what happened to the group.

IF

**They say it in front of everyone**

Usually during the signals segment, when the quoted caller lines are read aloud.

1. **Believe it out loud, first.** "That sounds like exactly what we have been describing." Before any advice.
2. Take the blame off them in a sentence addressed to the room rather than to them: these operations are staffed, scripted, and rehearsed against thousands of people.
3. **Do not ask for details.** Not the amount, not the bank, not what they said on the phone.
4. Offer the private route: "Can you stay after and we will go through it?"
5. Move on within about thirty seconds. Lingering turns the person into the exhibit.

IF

**They tell you privately afterwards**

The most common case, and the reason for staying ten minutes.

1. Listen first, and longer than feels necessary. Most people have not told anyone, and in this module many have not told their own family.
2. Watch for shame and name it directly: being taken in by one of these is not a failure of intelligence.
3. Give the referral and **describe what happens when they use it**, because a described service becomes an action and a web address stays a web address.
4. Suggest the freeze as the immediate step they can take today regardless of what else is true.
5. **Do not promise an outcome.** Whether money returns depends on how it left, and only the bank can answer that.

| | |
|---|---|
| IF<br>**Something else is going on**<br>Signs of coercion, confusion beyond the topic, or a family member who appears to be the source. | 1. **Do not investigate.** Do not question the person about their family, their finances, or their memory.<br>2. Do not confront anyone present.<br>3. Follow your organisation's escalation procedure, which you read before the session.<br>4. If you have no organisation behind you, know in advance which local agency handles adult protective concerns in your area, and have that number with you.<br>5. Record only what you observed, in your own words, without identifiers you were not given. |

NEVER, IN ANY BRANCH

- Never let anyone read a verification code, an account number, or a Social Security number aloud. Interrupt if it starts.
- Never write down or photograph anyone's identifiers, statements, or credit files, however much it would help you help them.
- Never log into anybody's account, dial on their behalf, or speak to their bank as them.
- Never give legal or financial advice. Naming who does is the correct answer and a complete one.
- Never promise that money comes back, that somebody will be caught, or that a report will be acted on.

### Why the restrictions are that strict

They look ungenerous on the page, and in the moment they will feel that way, because the person in front of you needs help and you could plainly give more of it. The reason to hold the line is that a volunteer holding somebody's credentials, or a note with their account number on it, has created a risk they cannot manage and a liability their host organisation did not agree to. It also puts you in the exact position the scheme in this module occupies, asking for the same things in the same reassuring voice, and participants notice that faster than you would expect.

What you can offer that nobody else in their week is offering is that you believed them immediately and you knew who to send them to. For most people that is the part that makes the call happen.

Room management

## What tends to go wrong in this session

None of these are unique to this module. All are more likely in it, because the subject attracts both strong feeling and confident misinformation.

LONG STORY

### The participant with a full account to give

Say, warmly: "I want to hear all of that, and I want to make sure everybody gets the phone numbers. Can you stay after?" Then move. Nearly everyone accepts, and the ones who stay needed the private conversation.

EXPERT

### The retired banker in the third row

If they are right, say so and thank them. If they are wrong, do not debate: "That is not what I have, and I would rather not give the room a number I am unsure about." Write it down visibly.

PUSHBACK

### "This is all fearmongering"

Take it seriously rather than defensively. Agree with the part that is right, which is that most calls are not fraud and most days nothing happens, then return to the specific.

DISTRESS

### Somebody becomes visibly upset

Stop the segment. Do not talk over it and do not spotlight them. Offer a break to the whole room, which lets them leave or compose themselves unwatched, then check privately.

PAPERWORK

### Someone hands you a statement to read

Look at it in their hands, without taking it and without writing anything down from it. Say what you would ask about and who to call. A real review is the referral's job, not yours.

UNKNOWN

### A question you cannot answer

Say you do not know, write it down in front of them, give the referral. Guessing produces confident misinformation that travels further than the session does.

### Things not to say in this module

× **"Never give out personal information."**
Too broad to act on and contradicted by everyone's daily experience. The rule here is narrow and teachable: a code you did not request, to anyone, ever.

× **"Just use a strong password."**
The scheme in the specimen defeats strong passwords, because it does not guess the password, it buys it from an old breach. Say what the code is for instead.

× **"Check your credit report and you'll be fine."**
Actively wrong for Track B, and the reason people believe they are covered when they are not. Checking is good. It is not sufficient.

× **A recommendation to buy monitoring.**
The free freeze does more than most paid products, and selling from the front of a room is not what you are there for.

× **A national loss figure you have not checked.**
Synthetic identity totals vary wildly by definition, partly because there is no victim to file a complaint. Say that instead.

× **"You should have known better."**
Including gentler forms: "didn't that seem odd?" A person who feels judged stops talking, and stops reporting.

### Questions that come up, and short answers

**Q I don't have much money. Why would anyone bother with me?**

Track B is not after their balance, it is after a Social Security number with a quiet history, which is worth more than a large balance. Say this plainly, because the belief is the main reason people skip the freeze.

**Q Will freezing my credit stop me getting a loan?**

Only while it is on. Lifting it is free, takes minutes, and can be done for a set window or a single lender. It does not affect the credit score.

**Q** **Does checking my own credit report hurt my score?**

No. Looking at your own file is recorded differently from a lender checking it for an application. This belief is common and it keeps people from looking.

**Q** **The caller knew my address and the last four digits of my card.**

That information is widely available from past breaches and bought cheaply. Knowing something about somebody is how the call earns trust, which is exactly why it is not evidence of anything.

**Q** **What about my grandchildren?**

A child's credit file can be frozen, and most parents have never heard that. Children's numbers are targeted because nothing is checked against them for fifteen years. Often the most useful thing a grandparent takes out of the room.

---

## Keeping it current

### What you send back keeps this accurate

This module is revised when the underlying detection work identifies new patterns, and when facilitators report what the room actually said. The second source will not exist unless somebody sends it.

The most valuable thing to report is not whether the session went well. It is the exact sentence a participant reported hearing from a caller, because that is a scheme variant arriving in a community room before it arrives anywhere it can be measured. Second most valuable is any number or web address you found out of date, because that failure will otherwise be repeated by every other facilitator using the same page.

> **WHAT TO SEND**
>
> Use the record on the following page, or simply write an email, to `[CONTACT]`. Send nothing that identifies a participant: no names, no account details, no credit files, no photographs. A count is enough where a count is relevant, and paraphrase anything a participant said rather than attributing it.

If you adapt the module, for a different region, language, or audience, that adaptation is worth sending too. The licence lets you change it freely and does not require you to tell anyone. It is simply useful if you do, so that the next facilitator with the same problem does not solve it again.

---

Form

### Delivery record

One page, printable. Fill it in immediately after the session while it is fresh. Nothing on it should identify a participant.

**Session record, Module 01**

Account takeover and synthetic identity · Complete after delivery · No participant identifying information

| | |
|---|---|
| DATE | |
| FACILITATOR | |
| HOST ORGANISATION | |
| LOCATION | Town and state is enough |
| IN PERSON OR VIRTUAL | |
| APPROXIMATE ATTENDANCE | |
| MINUTES USED | Full, or the 30 minute cut |
| HANDOUTS DISTRIBUTED | |
| CALLER LINES PARTICIPANTS REPORTED HEARING | Paraphrase the wording. This is the most useful line on the form. |
| QUESTIONS ASKED THAT THE MODULE DID NOT ANSWER | |
| NUMBERS OR WEB ADDRESSES FOUND OUT OF DATE | Which one, and what it did instead |
| HOW THE CREDIT FILE EXERCISE WENT | Which lines were flagged, including the legitimate ones |
| DISCLOSURES REFERRED ONWARD | A count only. No names, no details. |
| LIVE INCIDENT DURING SESSION | Yes or no. Nothing further. |
| SUGGESTED CHANGE TO THE MODULE | |

Afterwards

## What a session that worked looks like

Not applause, and not a room that looked interested. These are the observable things, and it is worth checking yourself honestly rather than kindly.

- [ ] Hands went up when you read the caller lines. If nobody recognised anything, you probably read them rather than said them.
- [ ] At least one person flagged a legitimate entry in the credit file, and left understanding why asking was still correct.
- [ ] Somebody could tell you the single action back in their own words without being prompted with the first half of it.
- [ ] At least one person said out loud that they were going to freeze their credit.
- [ ] Somebody stayed behind. An empty room afterwards more often means the session felt like a lecture than that nobody had anything to say.
- [ ] You said at least one honest "I do not know", and gave the referral instead.
- [ ] Nobody's private information was spoken aloud, written down, or photographed, including by you.
- [ ] You finished on the ending rather than running out of time before reaching it.

AND THE ONE THAT MATTERS MOST

The measure of this session is not what people know at the end. It is whether anyone hangs up on a call they would previously have stayed on, or freezes a file they would previously have left open. You will usually never find out. Deliver as if you will.

# Reuse, adapt, and teach this

This guide and the module it accompanies are published so that they can be delivered by people the author will never meet. Adapt the local numbers, translate them, change the specimen names, cut the session to thirty minutes. The only request is that the attribution stays on them, so that a participant who wants to check where the material came from can.

THIS GUIDE COVERS

- Module 01, account takeover and synthetic identity [LINK]
- Its participant handout [LINK]
- Other modules have their own guides

DERIVED FROM

Transaction fraud detection validated across approximately 1.9 million card records, its extension to a combined debit and credit environment, and the synthetic identity feature specification. [LINK] · [DOI]

REVISION

Version [VERSION], published [DATE]. Revised on new detection findings and on facilitator reports. Changelog: [LINK]

SEND CORRECTIONS AND RECORDS

[CONTACT]. Nothing that identifies a participant.

> Ayeni, A. [YEAR]. Facilitator guide, Module 01: account takeover and synthetic identity (Fraud prevention curriculum), version [VERSION]. [DOI] · Licensed CC BY 4.0.