MODULE 01: ACCOUNT TAKEOVER AND SYNTHETIC IDENTITY

The code is not the attack. It is the *alarm*

A 45 minute session on two schemes that both run on one piece of you: the people who take over an account you already have, and the people who build a new person out of your Social Security number. Written to be taught by a volunteer with no technical background.

TEXT MESSAGE, 11:42 PM — SPECIMEN, TEACHING MATERIAL ONLY

FROM: 34521

> Your verification code is
>
> **481 902**
>
> Do not share this code with anyone. If you did not request it, contact us.

NINETY SECONDS LATER. FROM: (404) 555 0148

> "This is the fraud department. We stopped a charge on your account. To confirm it's really you, read me the six digit code we just sent."

The first message is real. The bank did send it. It arrived because somebody already had her password and was standing at the login screen waiting for exactly one thing. The second message is the whole operation. The code was never a security check she had to pass. It was the last door, and she was being asked to open it from the inside.

AUDIENCE	RUN TIME	GROUP SIZE
Anyone with a bank account or a credit file Written for older adults and family caregivers	**45 minutes** 30 minute cut sheet included	**6 to 40** In person or virtual
FACILITATOR	**MATERIALS**	**VERSION**
Any trained volunteer No technical or banking background needed	**Handout and specimen credit file** Both included below, printable	`[VERSION]` Published `[DATE]`

LICENSE	ARCHIVED AT
CC BY 4.0 Copy, adapt, and teach it. Keep the attribution.	`[DOI]` Permanent identifier

Where this came from

This module is the back of a detection model, turned around

Nothing here is general advice about being careful. Every cue in this module is a measurement from a working fraud detection system, restated in the words of the person the fraud is aimed at.

Building a system that separates fraudulent transactions from real ones, or fabricated borrowers from real ones, requires describing a scheme in operational terms: what the person running it has to obtain, in what order, and what traces that leaves behind in the data. That description is what the model consumes.

Read it in the other direction and the same description says what the scheme looks like from the inside: what gets asked for, what pressure is applied, what a legitimate counterpart would never do. A detection feature and a recognition cue are two renderings of one analysis. The model uses it to score a transaction or an applicant. This module uses it to teach a person.

There is one thing this module has to be honest about, and it shapes everything that follows. Detection runs after an attempt has been made. It reduces loss and it does not prevent the approach. The only thing that stops either of these schemes before it starts is the person on the other end recognizing it, which is why this material exists at all.

> **THE FIXED STRUCTURE**
>
> Every module in this series uses the same four parts, in the same order, so that a volunteer who has taught one can teach any of them: **how the scheme works, the specific**

signals, the single action to take, and where to report. Everything after those four parts is delivery support.

Before you teach

What a participant can do at the end

Written as things a person does, not things a person knows. If a participant cannot do these five things after 45 minutes, the session did not work.

- [ ] Say in one sentence what a verification code is for, and why giving one away is different from giving away a password.
- [ ] Explain the difference between someone taking over an account they found and someone building a new account out of their Social Security number.
- [ ] Name the one action to take when a code arrives that they did not ask for, without needing to decide whether the caller is real.
- [ ] Describe what a credit freeze does, what it costs, and that lifting it is free and quick.
- [ ] Name the number or website they would use to start a recovery, and what they would have in front of them.

THE POINT OF THE SESSION

Participants leave with one habit and one setting. The habit is what they do when an unrequested code arrives. The setting is a freeze on their credit file. Almost everything else in this module supports those two.

01

How the schemes work

There are two here, and they are frequently taught as one thing, which is why people defend against the wrong one. Teach them separately. They take different things, they run on different timescales, and they are caught in different places.

TRACK A, FAST

Account takeover: they use the account you already have

Step 1

Get the password

Usually from a breach at some other company, bought in bulk. Reused passwords are why one old breach opens a current bank account.

Step 2

Hit the one remaining door

The password is not enough on its own. The account sends a code. That code is now the only thing standing between them and the money.

Step 3

Get you to hand it over

By phone, in the ninety seconds while the code is live, wearing the voice of the fraud department. Or by moving your phone number to their SIM so the code comes to them.

Step 4

Change the locks, then empty it

New email, new phone, new password. Your alerts stop arriving, which is the point. This is over in an hour.

TRACK B, SLOW

Synthetic identity: they build a person out of a piece of you

Step 1

Take a quiet number

A real Social Security number belonging to someone who does not use it much: a child, a retiree, someone who has not applied for credit in years.

Step 2

Attach a person who does not exist

A fabricated name, a plausible birth date, a real address. Every field checks out individually, because every field is real. Only the combination is false.

Step 3

Build ordinary credit, patiently

Small accounts, paid on time, for months or years. Sometimes helped along by being added as an authorized user on somebody's genuine, long standing account.

Step 4

Draw everything at once and vanish

Every limit maxed on the same day, nothing repaid. There is no person to pursue. The lender writes it off, and the number goes on to the next one.

Say this part out loud

Track A is loud and fast, and the participant will usually know within a day. Track B is the opposite, and this is the sentence the session exists to deliver: because the fake person carries a different name and a different birth date, the accounts they open do not appear on the participant's credit report. Watching your credit report is a real and useful habit, and it is not a defense against Track B, because there is nothing there to see.

What can be seen instead is indirect: mail arriving for a name nobody in the house recognizes, a collection call about a debt belonging to a stranger, or earnings on a Social Security statement from a job never held. Those are the traces that leak back to the real owner of the number.

The variants, as of this version

The fraud department call

PHONE, WITHIN A LIVE CODE WINDOW

The most common single approach. A caller who already has the password triggers a real code, then calls immediately and asks the participant to read it back "to verify your identity."

The pressure is time, and the time is genuine. The code expires in minutes, so the caller is hurrying because they actually have to.

The phone number takeover

CARRIER ACCOUNT, NO CONTACT WITH YOU AT ALL

The number is moved to a device the fraudster controls, so every code goes straight to them. Often done with information gathered beforehand, sometimes with an insider at a store.

The signal is unmistakable and easy to dismiss: the phone stops having service for no reason, in a place where it always works.

The password reset chain

EMAIL FIRST, THEN EVERYTHING ELSE

The email account is taken first because it is the master key. Every other account offers to reset itself through it.

Watch for mail rules that quietly forward or delete bank messages. The participant does not need to know how to check this, but should know to ask someone to.

The small test charge

CARD AND ACCOUNT FRAUD

A charge of a dollar or two at an unfamiliar merchant. It confirms the card is live before anything larger is attempted.

Participants routinely ignore these because the amount is trivial. The amount is trivial on purpose.

The unrequested new card

MAIL

A card, a welcome packet, or a change of address confirmation for an account nobody opened. Somebody applied in the participant's name and the mail reached the wrong address, which is to say the right one.

This is one of the few places where Track B becomes visible early. It should never be thrown away as junk.

Authorized user piggybacking

SYNTHETIC IDENTITY, CREDIT BUILDING

A fabricated person is added as an authorized user on a real account with years of clean history, and inherits enough of that history to look established.

The real account holder frequently never notices, because being an authorized user costs the primary holder nothing until the bust out.

Misuse of a child's or a late relative's number

SYNTHETIC IDENTITY, DORMANT NUMBERS

Numbers that will not be used for credit for years, or ever again, are the most valuable, because nobody is looking at them.

Grandparents in the room are frequently the right people to raise this with. A child's credit file can be frozen too, and most families have never heard that.

> **KEEP THE NATIONAL FIGURES SMALL**
>
> If a participant asks how big this is, resist quoting a total. Published estimates of synthetic identity losses vary widely and are built on different definitions, and the honest answer is that nobody has a precise number, partly because there is no victim to file the complaint. Say that, and move back to the specific. Overstating it costs credibility with the one participant in the room who knows better.

Derivation

One analysis, two renderings

Left: what the detection work measures in transaction and credit data. Right: the same fact, stated to the person it happens to. Facilitators do not teach the left column. It is here so that anyone can check that the right column was not invented.

WHAT THE MODEL MEASURES	WHAT THE PARTICIPANT IS TAUGHT
Deviation from the account's own baseline Amount, hour, merchant category, and location scored against what this particular account normally does, rather than against a fixed rule.	You are the baseline. A charge is suspicious because it is unlike you, not because it is large. Which is why a two dollar charge at a merchant you have never used matters more than a four hundred dollar charge at your grocery store.
Velocity across a short window Several attempts clustered in minutes, often across more than one channel, is a stronger signal than any single attempt.	When three things happen at once, that is the attack, not a coincidence. A code, an email about a password change, and a phone call, all inside ten minutes. That cluster is the moment to stop and do nothing quickly.
Class imbalance, minority class performance Fraud is under one percent of transaction volume. A model that calls everything legitimate scores 99% accuracy and catches nothing, so detection is measured on the rare class specifically.	Your bank is hunting for something rare, and it will sometimes miss. You are the backstop, not the first line. This is why "the bank would have caught it" is not a plan. Systems tuned to avoid stopping your real purchases will let some fraud through, by design.
Field validation versus behavioral pattern Every element of a synthetic identity is individually valid, so per field verification passes. Detection has to move to behavior across the credit lifecycle.	Nothing about the fake person is fake except the combination. That is why nobody caught it. And it is why the participant is not to blame for missing it either. The check the lender ran was the same check they would have run on you.

Credit history depth and file age at origination A file that begins abruptly, with no records before a recent date, distinguishes a constructed identity from an organic one.	This is why a quiet Social Security number is worth more than an active one. A number nobody is using has no history to contradict. Children, and adults who have not borrowed in years, are targeted for exactly that reason. It is not a judgment about them.
Revolving balance behavior and utilization Months of low utilization and clean repayment followed by simultaneous draw down across every line, then default. The bust out is visible only as a pattern over time.	The scheme is patient. Nothing looks wrong until all of it does at once. Which is why "I checked last year and it was fine" is not reassurance. Being fine is part of how it works.
Debt to income and delinquency patterning Across the credit behavior variable space, applications and inquiries precede accounts, so origination signals appear before repayment signals do.	An inquiry you did not make is the earliest thing you can see, and it arrives before the account does. Which makes the inquiries section of a credit report more useful than the accounts section, and almost nobody reads it.

Measurements above come from the transaction fraud detection work validated across approximately 1.9 million card records, its extension to a combined debit and credit environment, and the credit behavior variable space used in the loan modelling work. See `[LINK, reference implementation]` and `[LINK, feature specification]`.

02

The specific signals

Two sets, matching the two tracks. Set A is what an hour long takeover looks like while it is happening. Set B is what a scheme that has been running for two years leaves lying around the house.

Set A: signals during a takeover

CODE

A verification code you did not ask for

The single most important signal in this module. It means somebody is at the login screen right now, holding your password, waiting.

CALL

Someone calls about the code

No real institution will ever call and ask you to read one back. The code exists precisely so that nobody but you can use it.

PHONE

Your phone loses service for no reason

No bars, at home, with no outage. Your number may have been moved to somebody else's device, which means your codes are now going to them.

EMAIL

Notices that a detail was changed

Email address updated, phone updated, password reset, new device signed in. Especially if several arrive together, and especially at night.

QUIET

Alerts that used to arrive have stopped

Silence is a signal too. The first thing a takeover does is redirect the notifications so you stop hearing about it.

SMALL

A charge too small to bother with

A dollar or two somewhere unfamiliar. It is a test to see whether the card works and whether anybody is watching.

Set B: signals that a number is being used elsewhere

MAIL

Mail for a name nobody here recognizes

Statements, offers, or collection letters addressed to a stranger at your address. This is often the only visible trace of a synthetic identity.

MAIL

A card or welcome packet you did not apply for

Somebody applied using your details and the mail came here. Do not shred it and forget it, because it is evidence with a date on it.

CALLS

Collectors chasing a debt that is not yours

Particularly for a name that is not quite yours. Ask which name and which address they have on file, and write down the answer.

CREDIT FILE

Inquiries from lenders you never approached

The earliest visible sign. An application leaves a mark before an account does, so the inquiries section shows things the accounts section has not caught up with.

CREDIT FILE

An address or an employer you never had

The personal information section is the one people skip. A false address attached to your file is how somebody else's mail becomes your problem.

EARNINGS

Earnings on your Social Security record from a job you never held

Somebody used the number to work. Worth checking once a year, and almost nobody does.

Lines participants report hearing

Read two or three aloud. Recognition of the exact phrasing does more work than any list of principles.

> *"I'm calling from the fraud department. Read me the code we just sent so I can confirm it's you."*
>
> The one sentence that matters. Nobody legitimate says it, ever.

"Do not hang up. If you hang up, the transfer will go through."

Hanging up is the correct move and they know it, which is why they say this.

"We need to move your money to a secure account while we investigate."

There is no such thing. Banks do not ask customers to move money to protect it.

"Press one to approve, or press two to decline this charge."

The automated version. Pressing anything at all confirms the number is live and connects you to a person.

"This is Microsoft support. We've detected activity on your account."

The route to the email account, which is the master key to all the others.

03

The single action

One action, taught as a reflex, because deciding whether a caller is legitimate is the part people get wrong. The action is designed to work without that decision.

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.

Nobody legitimate will ever ask you to read a verification code aloud, type it into a phone keypad, or forward it in a message. There is no exception, no department, and no emergency that makes it necessary. That is what allows this to be a reflex rather than a judgment: the participant never has to work out who is calling, because the answer is the same either way.

The next ten minutes, if a code arrives unrequested

1. Say nothing and end the call, if there is one. You do not owe anybody an explanation, and staying on the line is what the caller needs.
2. Go to the account yourself, through the app or the number on the back of your card. Never a number, link, or address supplied by whoever contacted you.
3. Change the password on that account, and on your email if the password was shared between them.
4. Check whether the email address or phone number on the account was changed. That change, not the missing money, is the sign that somebody is inside.
5. If your phone has lost service, use somebody else's phone and call your mobile carrier first. Until the number is back, every code is going to the wrong person.

> **AND ONE SETTING, ONCE**
>
> Freeze the credit file at all three bureaus. It is free by federal law, it blocks new accounts from being opened in the participant's name, and it can be lifted in minutes when they actually want credit. It is the only measure in this module that works against the slow scheme, because it stops the fake person from opening anything at all.

> **IF MONEY HAS ALREADY MOVED**
>
> Speed changes the outcome here more than in most fraud, so a participant who realizes mid session should be encouraged to call their bank before the session ends rather than after. Ask for the fraud department, say the words "unauthorized transaction," and write down the time of the call and the name of the person. Do not promise them the money will come back. Whether it does depends on how it left, and that is a question for the bank.

04

Where to report

Give the whole list on the handout, but say one number out loud and repeat it. Participants who leave with eight numbers call none of them.

REPORTING AND RECOVERY CHANNELS. CONFIRM EVERY NUMBER IS CURRENT BEFORE EACH DELIVERY.

WHO	CONTACT	USE IT FOR
Your own bank or card issuer	**The number on the back of the card** Never a number from a call, text, or search result	Always first when money has moved or an account is compromised. Ask for the fraud department. Write down the time and the name of the person you spoke to.
Federal Trade Commission	**1-877-438-4338** IdentityTheft.gov	The one to say out loud. It produces a personal recovery plan, the letters to send, and the sworn identity theft report that banks and

WHO	CONTACT	USE IT FOR
		bureaus ask for. Free.
Equifax	**1-800-685-1111** equifax.com	Credit freeze, free by federal law. Freeze all three bureaus, not just one, because lenders do not all use the same bureau.
Experian	**1-888-397-3742** experian.com	Credit freeze, free. Also where a fraud alert can be placed, which is weaker than a freeze but propagates to the other two automatically.
TransUnion	**1-888-909-8872** transunion.com	Credit freeze, free. A freeze can also be placed for a child or for an adult whose affairs the participant manages.
Your credit reports	**AnnualCreditReport.com** 1-877-322-8228	The only federally authorized source for free

WHO	CONTACT	USE IT FOR
		reports from all three bureaus. Read the inquiries and the personal information sections, not only the accounts.
Social Security Administration	**1-800-269-0271** Office of the Inspector General, ssa.gov	Reporting misuse of a Social Security number, and checking the earnings record for work the participant never did.
Your mobile carrier	**Store or customer service** Ask for a port out PIN or number lock	Immediately if the phone loses service unexpectedly, and in advance as prevention. A number lock is the single best defense against code interception.
AARP Fraud Watch Network Helpline	**877-908-3360** Free to anyone, member or not	Talking it through with a trained volunteer, including when

WHO	CONTACT	USE IT FOR
		the person is not ready to file anything yet.

TWO THINGS TO CORRECT IN ADVANCE

Participants believe a freeze costs money or hurts their credit score. It does neither. It is free by federal law at all three bureaus, it does not affect the score, and lifting it temporarily takes minutes online or one phone call.

Participants confuse a freeze with a lock. A freeze is the free legal right. A lock is a product some bureaus sell, sometimes bundled with a subscription. Point participants at the freeze and be plain that nobody needs to buy anything today.

Delivery

Forty five minutes, timed

Timings are the version that survives contact with a real room. If you are running long, the cut is marked below. Cut it rather than compressing the exercise.

0:00 to 0:04	**Open with the message, not the topic** Read the two specimen messages aloud, the bank's and then the caller's, ninety seconds apart. Ask: "Which one of these is fake?" Most rooms say the first. The answer that lands is that the first one is real, and that is exactly why it worked.
0:04 to 0:14	**The two tracks** Walk Track A, then Track B. Keep them visibly separate on the board. The single most valuable minute in the session is the one where you explain that the fake person's accounts do not appear on the participant's 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."*
0:14 to 0:21	**The signals** Read three of the quoted lines aloud in the caller's voice. Ask who has heard something close to one of them. Hands will go up, and that is the moment the room engages. Cover Set A quickly. Spend the time on Set B, because those signals arrive as ordinary mail and get thrown away.
0:21 to 0:32	**Exercise, read the specimen credit file** Hand out the specimen. Four minutes in pairs or alone: circle anything you would ask about. Then take answers from the room before revealing. Take wrong answers seriously. Two of the unfamiliar lines are legitimate on purpose, and somebody flagging them is the teachable moment, not a mistake.
0:32 to 0:38	**The one action, and the one setting** State the action once, plainly. Then have the room say it back. Then walk the freeze: three bureaus, free, lift it in minutes. > *"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."*

0:38 to 0:43	**Where to report** Hold up the handout, point at IdentityTheft.gov and the number beside it, and say what it gives them: a plan written for their situation, and the sworn report that banks ask for. One number said aloud beats nine numbers printed.
0:43 to 0:45	**Close, and stay in the room** Close on the freeze being free and reversible. Then say you will stay for ten minutes, and stay. Most disclosures happen after the session ends, not during it. Leaving promptly costs the session its most important conversations.

THE 30 MINUTE CUT

Drop the variant list to three (fraud department call, phone number takeover, 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 is a session that leaves people worried and unequipped.

Exercise

The specimen credit file

Seven entries from one report. Three of them should not be there. Participants mark what they would ask about, and the facilitator reveals afterward. On screen, select a line to see the answer. On paper, the answer key is on the back.

SPECIMEN, TEACHING MATERIAL, NOT A REAL REPORT

ACCOUNTS, INQUIRIES, AND PERSONAL INFORMATION

Consumer credit file, extract

File for: **Ruth A. Whitfield** (fictional) · Reports like this are free from all three bureaus at AnnualCreditReport.com.

DATED	ENTRY	BALANCE OR TYPE
Opened 2009	Credit card. FIRST MERIDIAN BANK, N.A.	$412.00

This one is fine.

Her own card, opened years ago, small balance, paid monthly. Include lines like this so participants practice distinguishing rather than flagging everything.

Opened 2016	Retail card. COMENITY CAPITAL BANK / GARDEN HOUSE	$0.00

Unfamiliar name, legitimate line.

She remembers the store card, not the bank behind it. Store cards are almost always issued by a bank whose name never appears in the shop, so the credit file shows a name the customer has never seen.

This is one of the two most useful lines in the exercise. An unrecognized name is a reason to ask, not a reason to conclude.

Opened Mar	Personal line of credit. HARBORLINE LENDING GROUP	$9,800.00

Ask about this one.

She did not open it, has never heard of the lender, and the balance is close to the limit within four months of opening.

An open account she did not create is the clearest form of this. It goes to the bureau as a dispute and to IdentityTheft.gov for the sworn report, and the freeze goes on the same day.

Closed 2021	Auto loan, paid in full. LAKESIDE FEDERAL CREDIT UNION	$0.00

Fine, and worth a sentence.

Closed accounts stay on a report for years after they are paid off. Participants often think an old settled loan showing up is an error. It is not, and a closed account in good standing is helping them.

DATED	ENTRY	BALANCE OR TYPE
Feb 04	Inquiry. PINEGATE AUTO FINANCE (application for credit)	**Hard inquiry**

Ask about this one.

She has not applied for anything. Somebody submitted an application in her name, and this mark appeared before any account did.

Inquiries are the earliest visible signal and the section everybody skips. Point out that this one is dated weeks before the Harborline account was opened, which is what an attempt and then a success looks like in sequence.

On file	Address on file: 1140 SOUTH VERNON AVE, APT 6	**Personal info**

Ask about this one.

She has never lived there. An address she does not recognize attached to her file is how somebody else receives mail issued in her name, and how a fabricated person borrows the legitimacy of her record.

Distinguish this from the next line carefully. A wrong address is a problem. A differently formatted version of a real address is not.

On file	Name on file: RUTH ANN WHITFIELD; also R A WHITFIELD	**Personal info**

This one is fine.

Bureaus keep every version of a name that lenders have reported over the years, including initials, maiden names, and misspellings. Variations of her own name are normal.

The line that matters is a name that is not a version of hers at all. That is the synthetic identity signal, and it is worth saying out loud so the room can tell the two apart.

Three entries should not be there. Two are unfamiliar but legitimate.

RUNNING IT WELL

Take answers from the room before revealing anything, and write every flagged line on the board including the wrong ones. Then reveal. The session lands when a participant

> sees that their instinct on the store card was reasonable and that the answer was a phone call rather than a judgment.

Facilitator notes

Someone in the room has already been through this

In a group of thirty older adults, assume it. This module attracts more shame than the others, because the participant handed something over rather than merely failing to notice something. How that is handled matters more than the rest of the session.

Someone will say, out loud or afterward, that this happened to them. What happens next matters more than the rest of the session.

- [ ] **Believe it and say so first.** "That sounds like exactly what we've been describing" does more than any advice that follows.
- [ ] **Name the design, not the person.** These operations are staffed, scripted, and rehearsed against thousands of people. Say that early and say it to the room, not only to the person who spoke.
- [ ] **Do not ask for details in front of the group.** "Can you stay after and we'll go through it?" moves it somewhere private without dismissing it.
- [ ] **Never let anyone read a code, an account number, or a Social Security number aloud.** Say it plainly if it starts to happen. There is no version of this session where any of those is spoken in a room.
- [ ] **Do not write down or photograph anyone's account details, and never log into anyone's account for them.** You are not their representative. Handling somebody's credentials creates a risk you cannot manage and a liability you do not want.
- [ ] **Do not tell them whether the money is coming back.** It depends on how it left, and the bank is the only party who can answer it. Say you do not know.

- [ ] **If it is live, treat it as urgent.** Somebody who realizes during the session that their phone lost service this morning should be calling their carrier now, not after. Help them step outside and do it.

- [ ] **Hand them IdentityTheft.gov and describe what it produces.** A recovery plan for their situation and a sworn report that banks and bureaus accept. Making it concrete is what turns it into an action.

- [ ] **Follow your organization's escalation guidance** where there are signs of coercion, cognitive decline, or possible financial exploitation by a family member. Know what it says before you deliver the session, not after.

×

Too broad to act on, and participants give out personal information all day. The rule is narrow and teachable: a code you did not request, to anyone, ever.

×

The scheme in the specimen defeats strong passwords, because it does not guess the password, it buys it. Say what the code is for instead.

×

Actively wrong for the synthetic identity track, and the reason people believe they are covered when they are not. Checking is good. It is not sufficient.

×

The free freeze does more than most of them. Suggesting a purchase from the front of a room also puts your organization somewhere it should not be.

×

Do not walk a room through changing security settings on devices you cannot see. Name what to do and who can help them do it.

×

Including in gentler forms, such as "didn't that seem strange?" A person who feels judged stops talking, and stops reporting.

Print the handout at 14 point or larger. Say every phone number twice, slowly, and write it where it can be seen. Never rely on the red marks alone to carry meaning, and say which lines are the problem. Face the room when you speak, because a facilitator reading from a screen with their back turned is inaudible to a significant part of any older audience. Assume some participants do not use a smartphone at all, and note as you go that every step in this module can be done by telephone.

Q

The synthetic identity track is not after their balance. It is after a Social Security number with a quiet history, and a quiet history is worth more than a large balance. Say that plainly, because this belief is the main reason people skip the freeze.

Q

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

Q

No. Looking at your own file is recorded differently from a lender checking it for an application, and has no effect on the score. This belief is common and it keeps people from looking.

Q

No, and this is worth answering carefully. That information is widely available from past breaches and is bought cheaply. Knowing something about someone is how the call earns trust, which is exactly why it is not evidence of anything.

Q

A child's credit file can be frozen, and most parents have never heard that it can. Children's numbers are targeted because nothing will be checked against them for

fifteen years. This is often the most useful thing a grandparent takes out of the room.

Q

Say you do not know, write it down in front of them, and point them at IdentityTheft.gov or the AARP helpline. Guessing in a session like this produces confident misinformation that travels further than the session does.

Take home

Participant handout

One page, plain language, printable at large type. This is the part that leaves the room, so it carries the action, the setting, and the numbers, and nothing else.

A code you did not ask for is a warning, not a request

One habit, one setting, and the numbers to call if something has already happened.

The habit

- **Never read a verification code to anyone.** Not aloud, not typed into a keypad, not forwarded. No real bank, shop, or government office will ever ask.
- If a code arrives that you did not request, somebody already has your password and is at the login screen right now.
- End the call. You do not owe anyone an explanation.
- Then go to the account yourself, using the app or the number on the back of your card.
- If your phone suddenly has no service at home, call your mobile company from another phone straight away.

The setting

- **Freeze your credit at all three bureaus.** It is free by law.
- It stops new accounts being opened in your name. It does not affect your credit score.
- Lifting it takes minutes when you actually want to borrow.
- A freeze is the free legal right. A lock is something a company sells you. You do not need to buy anything.
- You can freeze a file for a grandchild, or for someone whose affairs you manage.

Things not to throw away

- Mail for a name nobody in the house recognizes.
- A card or welcome packet you never applied for.
- A letter from a collector about a debt that is not yours.
- A charge of a dollar or two you do not recognize. Small charges are tests.
- An email saying your address or phone number was changed, when you did not change it.

START WITH THIS ONE

IdentityTheft.gov · 1-877-438-4338

Federal Trade Commission. Free. It builds a recovery plan for your situation and produces the sworn report banks and credit bureaus ask for.

Freeze your credit

- **Equifax:** 1-800-685-1111
- **Experian:** 1-888-397-3742
- **TransUnion:** 1-888-909-8872
- All three. Lenders do not all use the same one.

Check what is on file

- **AnnualCreditReport.com** or 1-877-322-8228, free from all three bureaus
- Read the **inquiries** and **personal information** sections, not only the accounts
- **ssa.gov** to check your earnings record for work you never did

If something has happened

- **Your bank:** the number on the back of your card, never a number from a call
- **Social Security misuse:** 1-800-269-0271
- **Your mobile company:** ask for a port out PIN or number lock
- **AARP Fraud Watch Helpline:** 877-908-3360

Reuse, adapt, and teach this

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

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. Reference implementation: [LINK] · [DOI]

REVISION

Version [VERSION], published [DATE]. Revised when the detection work identifies new scheme patterns. Changelog: [LINK]

CORRECTIONS

Report an error, an out of date phone number, or a scheme variant this module does not cover: [CONTACT]

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