# 1-3: How to Protect Your Identity

| | |
|---|---|
| Cast List<br>• Terri<br>• Security Specialist, 40s, black or Hispanic female, Antonia Lopez<br>• ID Theft Victim, mid-to-late 20s, white female, Marsha<br>Synopsis<br>• Terri and Security Specialist meet ID Theft Victim, who's had her wallet stolen recently<br>• They discuss types of ID theft, safeguards, what to do<br>Location<br>• Inside a Caffeine Station café, a busy Starbucks-type coffee shop | A. Identity Theft Overview<br>a. Definition of identity theft<br>b. The impact of identity theft<br>B. Identity Theft – Personal Property<br>a. Pockets, wallets, and purses<br>b. Mailbox<br>c. Trash<br>d. Checks<br>e. Driver's license<br>C. Preventing Identity Theft of Personal Property<br>a. Bring only what you need for the day<br>b. Protect key information: SSN, account & card numbers<br>i. Do not print them on checks<br>ii. Use alternate # instead of driver's license<br>iii. Shred bank statements (crosscut shredder)<br>c. For mail<br>i. Locked mailbox or PO box<br>ii. Mail bills in Postal Service boxes/post offices<br>iii. Direct deposit<br>D. Identity Theft – Electronic and Remote<br>a. Online<br>i. Phishing<br>ii. Pharming<br>b. Telemarketing<br>E. Preventing Electronic and Remote Identity Theft<br>a. Legitimate banks, merchants won't request SSNs or acct. numbers online or by phone<br>i. Contact organizations through regular channels to verify<br>ii. Find out how personal info will be used even by legitimate organizations<br>iii. National Internet Fraud Watch Information Center, www.fraud.org; 800-876-7060<br>b. For computers<br>i. Don't open unknown attachments<br>ii. Firewalls<br>iii. Patches<br>iv. Passwords<br>v. Federal Trade Commission's website at www.ftc.gov/infosecurity<br>c. Review statements and credit reports regularly<br>i. How to obtain<br>ii. What to look for<br>iii. If eligible, place "active duty alert" in credit report<br>F. If You Suspect Identity Theft<br>a. Immediate steps<br>i. Initial fraud alert<br>ii. Order and review credit reports<br>iii. Create an identity theft report<br>1. File an FTC complaint<br>2. File a police report<br>b. Keep records<br>c. Consider extended fraud alert<br>d. Report errors<br>i. To credit reporting agencies<br>ii. To businesses<br>iii. To ATM and debit card issuers<br>iv. To checking accounts<br>v. To credit card issuers<br>e. 1-877-IDTHEFT or www.FTC.gov/IDtheft<br>G. Opting Out<br>a. How it can protect your identity<br>b. How to opt out<br>c. What banks can and cannot share<br>d. Privacy notices |

*Theme music up*

*Darryl is in the studio.*

DARRYL: This is…the "Money Smart Podcast Network with Darryl and Terri."

*Music down*

DARRYL: This podcast series was created to help you know more about money and banking. We're addressing some of your most pressing questions, and we're talking to experts who can help give us some answers and understanding.

TERRI: *(from remote; breaking in)* Hey, did you say "*Darryl* and Terri?"

DARRYL: *(sound of him hurriedly turning off her microphone)* Oooops. Oh what sorry Terri I couldn't hear you there, technical difficulties. Uh…so. We've been getting letters from listeners like you asking for advice on some money-related matters. And we're bringing in experts to help us understand the topics and answer questions. *(to Terri)* Uh, Terri. Are you there?

TERRI: *(somewhat mock annoyed)* Well, I was. Until you shut off my mic. But, yes, I'm back now.

DARRYL: I was just going to introduce the topic.

TERRI: That sounds like a good idea.

DARRYL: So today we're beginning with a question we got from Marsha, a listener from Eureka, California. She's concerned about identity theft. Here's what she said.

MARSHA: *(playback of the message she left on the show's voicemail; it should be read in a slightly stilted manner, as a non-actor would when reading something out loud)* "Dear Terri and Darryl—"

DARRYL: *(breaking in)* She means, "Darryl and Terri."

MARSHA: *(playing back)* "My wallet was stolen recently. I cancelled my credit cards as soon as I noticed, and got new ones. Was that all I should have done? Plus, it started making me really nervous about identity theft. What can I do to protect myself?"

DARRYL: Those are fantastic questions. To answer them, Terri is on a field trip to Marsha's hometown of Eureka, California, along with security consultant Antonia Lopez, an authority on identity theft. *(to Terri)* Terri, are you there?

*"Coffee house" sounds in the background throughout. We hear the clinking of cups, a barista's now-and-again faint calls of: "triple-foamed non-fat extra-hot raspberry espresso with a whip" and so on*

TERRI: Yup. Haven't gone anywhere Darryl. *(to listeners)* So we're visiting Marsha at what we're told is one of her favorite hangouts – the Caffeine Station. From the looks of it – and I imagine the sound of it – it's the favorite hangout of at least half of her college classmates, too.

*Initial sounds of Marsha typing on her laptop as Terri and Antonia go up to introduce themselves.*

TERRI: Good morning. Marsha? I'm Terri, from the "Money Smart Podcast Network."

MARSHA: Yes, oh, wow – you're from the radio! I didn't expect you to come here!

TERRI: Well, here I am, and I've brought with me an expert to help you with your identity theft questions. Do you have 10-15 minutes this morning to talk with us on the air?

MARSHA: Uh, I have to leave for class in about 15 minutes…

TERRI: That's perfect, because you have the quick-witted, fast-talking half of our team here.

*They laugh*

TERRI: Marsha, this is Antonia Lopez. She was on the police identity theft teams of three cities in Michigan and Illinois over the past 10 years. She worked alongside federal investigators on some cases. Now she's a private consultant who specializes in identity theft.

MARSHA: Hi!

ANTONIA: *(it's ok if Antonia sounds a little rough around the edges; she was a cop)* It's good to meet you.

TERRI: Antonia's going to help you and our listeners learn to protect ourselves.

ANTONIA: Basically, I've seen it all. All the tricks, all the tactics, you name it.

TERRI: Marsha, why don't you start by telling Antonia what happened with your wallet.

MARSHA: Well, about two weeks ago I was sitting, uh… *(her voice changes slightly, because she's craning her neck)*…over there. On the green couch. I was working on a paper. I reached into my purse for my wallet, and it wasn't there. I looked all over. Gone.

ANTONIA: It can happen so fast, right? In the future, keep your purse on your lap, not beside you, since it's easy to be distracted.

TERRI: And men?

ANTONIA: It's safer to carry wallets in an inner jacket pocket, or front pants pocket so it's harder for a thief to take.

ANTONIA: I was told that you cancelled your credit cards right away. Is that right, Marsha?

MARSHA: Yeah. And my ATM card, too. But whoever took it managed to charge $1,000 on one of my debit cards anyway.

ANTONIA: Well, you did the right thing. You need to notify those banks within two business days. That way the most you might be responsible for is $50.

MARSHA: Wow! Fortunately they didn't ask me to pay anything. What if you call them *after* two days?

TERRI: You might lose up to $500, or perhaps much more.

MARSHA: No way!

TERRI: Let's move on to identity theft.

ANTONIA: Right. If it was just your credit cards and ATM card and you cancel them right away, that's one thing. Think about what else was in your wallet. Did the thieves get other personal information from your wallet like your birth date, social security number, or bank account?

MARSHA: No, that day I just had my credit cards and some cash.

TERRI: That's a relief!

ANTONIA: Good. I always recommend that people carry only what they need for the day. It's never a good idea to carry around your social security card. Keep it secured at home, along with any credit cards you're not using or put it in a safety deposit box. You need to be aware, though, that this kind of information is very valuable to thieves. They can use it to open new accounts in your name. And they'll take it from anywhere they can, whether that's your pocket or purse or even from your mailbox. They will even go through your trash to find it.

MARSHA: Yuck!

ANTONIA: So don't print your social security number on your checks, or use it on your driver's license. Also be careful with bank statements or any documents with personal information. That's what thieves are after in your trash.

TERRI: You know… I think Darryl's favorite jacket came from a dumpster. There's a reason we leave him at the studio. Antonia, you had suggested I get a shredder.

ANTONIA: Yeah. That's the best way to deal with bank statements or other mail that has your social security number or your account number on it. File it safely if you need to keep it – and shred it when you don't. Make sure it's a *crosscut* shredder. That makes it almost impossible to put documents back together.

TERRI: To stop getting many of those credit card offers altogether, you can do what's called "Opt Out."

MARSHA: What's that?

TERRI: It's taking yourself off of the mailing list for offers of credit or insurance. It gives thieves fewer opportunities to try to open a credit card in your name.

ANTONIA: That means your mailbox is less attractive to thieves.

MARSHA: That sounds good!

TERRI: It's easy, too. Just call 1-888-OPT-OUT (1-888-567-8688) or fill out the form at www.optoutprescreen.com.

ANTONIA: Marsha, the thief didn't get a driver's license from you, right?

MARSHA: Right.

ANTONIA: That's also good. If he had, he'd know where you live. I would recommend that if your mailbox didn't have a lock, get one that does or get a post office box. Use direct deposit if your employer offers it.

MARSHA: I guess I was really lucky!

TERRI: Definitely.

ANTONIA: And…and this has been bothering me since we came in. *(hear "thud" sound of Antonia closing Marsha's laptop)* Your private information can be stolen online if you're using a public computer, post the wrong information on social media, or respond to a fake e-mail or text message.

MARSHA: Aw! But this is my own computer.

ANTONIA: But have you secured your computer by installing antivirus software and firewall protection?

MARSHA: Yes!

ANTONIA: And do you have it set to update automatically?

MARSHA: Oh, I don't think I do! And I was buying and downloading music here all the time!

TERRI: One big problem is a fake e-mail or text message that looks like it came from your bank or credit card company – or even an online seller. It'll usually say something like there's a problem, and you need to verify your account information, password, and credit card or they'll have to suspend your account.

ANTONIA: That's called a "phishing" scam—

MARSHA: —as in…flounder?

TERRI: No, this phish is spelled with a "PH" at the beginning.

ANTONIA: It happens by phone, too. Another scam is pharming –

MARSHA: Let me guess: this farm has nothing to do with the place where they grow spinach.

TERRI: Correct. It's also spelled with "PH" – I don't know why they do that!

MARSHA: Phun times.

ANTONIA: Pharming is when the e-mail directs you to a website that looks like it belongs to an online merchant or bank you do business with.

MARSHA: So how do you know if it's real or phake? *(to Terri)* I said that with a "PH."

ANTONIA: The big point is no *real* bank or business will ask for that kind of information in an e-mail or a phone call. So don't provide any information over the phone or e-mail. Don't click on any links, or open any attachments.

TERRI: If you're unsure, you can call the bank's customer service number listed on your credit or debit card, which you know is real. That way you can make sure there are no issues with your account.

ANTONIA: You can also contact the National Fraud Information Center by going to www.fraud.org. That site lets you report suspicious e-mails and calls asking for personal information. It has a lot of great information, too.

TERRI: For our listeners, are there other steps Marsha should have taken when her wallet was stolen?

ANTONIA: Marsha, you were right to contact your credit card companies and report the stolen cards. If any checks had been taken, you might have considered opening new checking and savings accounts and stop payment on the missing checks. A new ATM card and PIN would be a good idea.

MARSHA: Um…now that I'm thinking about it, I couldn't find my driver's license this morning – maybe they did take it. I can get a duplicate, but…how do I know if someone is using my information?

ANTONIA: First, if you haven't reported the theft to police, do so and keep a copy of the police report.

Next, be sure to look at all your bank and credit card statements as soon as they're available. Check for any purchases you didn't make, or new credit cards or loans you didn't request. If you see anything suspicious, report it immediately to security or fraud department of your bank or credit card company.

You also can contact a check verification company, who will notify stores not to accept the stolen checks. Two that work with consumers are TeleCheck and Certegy.

TERRI: You can find specifics for those companies in the InfoBooth portion of the Money Smart Podcast Network, at www.fdicmspodcast.com.

ANTONIA: Next, get and look at your credit reports. By law you can get a complete and free credit report every twelve months from each of the three major credit reporting agencies. Those are Equifax, Experian, and TransUnion. You can request a report online at www.annualcreditreport.com

TERRI: This information is also at www.fdicmspodcast.com.

MARSHA: Whoa, I'm getting a little lost.

ANTONIA: I'm going fast so you can get to class. Just remember that there's complete information on all this at www.fdic.gov, under the Consumer Protection section, so you can follow up on everything.

TERRI: It is a good resource. Other questions, Marsha?

MARSHA: What do I do when I get my credit report?

ANTONIA: Check for any new loans or credit accounts that you didn't request. If you see anything suspicious, contact the fraud department of any of the credit reporting agencies. You can find details at www.ftc.gov/idtheft. You'll want an initial fraud alert placed in your credit file; that alert will last for 90 days.

MARSHA: Ok.

ANTONIA: In fact, to be really safe, you can ask to have an initial fraud alert put on your file even before you get your credit report. It tells potential creditors to take extra steps when you – or someone pretending to be you – tries to open an account in your name.

TERRI: And there's an extended fraud alert too, right?

ANTONIA: Right. Marsha, that's if you become a victim of identity theft. It lasts for seven years. Potential creditors have to take even more steps before they open an account for you.

TERRI: I know this isn't your situation, Marsha, but I always like to tell people that if you know any active military personnel, you should tell them about "active-duty alert."

ANTONIA: Right. It tells potential creditors to take extra steps when opening accounts for those on active military duty.

TERRI: We're running out of time… any last advice for Marsha?

ANTONIA: Marsha, best of luck. And if you wind up talking to or corresponding with your creditors, the police, or the credit reporting agencies, keep good records. And quickly complete any of the steps you haven't done – it can make a big difference in avoiding problems later.

MARSHA: Antonia and Terri, thank you so much!

TERRI: Antonia, thank you for sharing so much great information on identity theft.

ANTONIA: Any time.

*Theme music up*

TERRI: Well, that's it from the Caffeine Station in Eureka, California. This has been the "Money Smart Podcast Network, with Terri and Darryl."

DARRYL: Eureka! It's *Darryl* and Terri.

TERRI: You did NOT just say that.

*Music fades*