PFL Academy

Teacher Guide: Chapter 6.4 — Identity Theft Prevention and Recovery

OVERVIEW

TIME	MATERIALS	PREREQUISITES
45-50 Minutes	Student Activity Packet	Consumer Fraud Protection (L-28)

LESSON FLOW

5 min — **THE CHALLENGE**

- Read Maria's credit card fraud scenario aloud.
- Ask: "How would you feel discovering $3,000 in charges you didn't make?"
- Discuss: How might her information have been stolen?

10 min — **CORE CONCEPTS**

- Distinguish between credit freeze (blocks new accounts) and fraud alert (warns creditors).
- Categorize theft methods: digital (phishing, data breaches) vs. physical (skimming, mail theft).
- Emphasize: FTC reports 200+ hours needed to resolve identity theft—prevention is critical.

25-30 min — **APPLY IT**

- **Part A (12 min):** Scenario analysis—identify tactics and prevention strategies.
- **Part B (8 min):** Warning signs table—connect signs to meanings and actions.
- **Part C (10 min):** Recovery sequencing and personal protection checklist.

10 min — **CHECK YOUR UNDERSTANDING**

- Review Q1—credit freeze vs. fraud alert distinction.
- Discuss Q3—proper sequence of Maria's recovery steps.
- Share Q5 reflections on overlooked protection measures.

DIFFERENTIATION

Support

- Provide a visual flowchart of recovery steps.
- Use a T-chart comparing digital vs. physical theft methods.
- Pre-fill one row of the warning signs table as an example.

Extension

- Research synthetic identity theft and how it differs from traditional theft.
- Create an identity protection guide for family members.
- Investigate the Identity Protection PIN program from the IRS.

ANSWER KEY

Part A: Identity Theft Tactics Analysis

Scenario 1: PHISHING. Red flags: Urgent deadline, request for SSN/password, link to click. Protection: Never click links in unsolicited emails; contact bank directly through official website or phone number on card.

Scenario 2: SKIMMING. Red flags: Card used at unattended payment terminal. Protection: Inspect card readers for loose parts, use tap-to-pay when available, prefer credit over debit for better fraud protection.

Scenario 3: DUMPSTER DIVING. Red flags: Documents with personal information in trash. Protection: Shred all documents with personal info, opt out of pre-approved credit offers at OptOutPrescreen.com.

Part B: Warning Signs Table

Unexpected credit denial: Someone may have damaged your credit. ACTION: Request free credit report immediately.

Bills stop arriving: Thief may have changed your address. ACTION: Contact creditors and check with USPS.

Unfamiliar accounts: New accounts opened in your name. ACTION: Contact creditor, freeze credit, file FTC report.

Collection calls: Debts from fraudulent accounts. ACTION: Request debt validation, file police report.

IRS duplicate return: Tax identity theft—refund already claimed. ACTION: File Form 14039, contact IRS.

Part C: Recovery Action Plan

4. Correct order: (1) Call affected companies, (2) Place fraud alert, (3) File FTC report, (4) File police report, (5) Change passwords/PINs, (6) Continue monitoring.

> *Good checklist items: Use strong unique passwords, enable two-factor authentication, shred sensitive documents, check credit reports regularly, use credit monitoring, freeze credit when not needed, be cautious on public Wi-Fi.*

Check Your Understanding

1. B (A credit freeze blocks new credit inquiries; a fraud alert warns creditors to verify identity)

2. To claim the victim's tax refund. The thief files early with false income information and steals the refund before the real taxpayer files.

3. (1) Call credit card company to report fraud and cancel card, (2) Review other accounts for suspicious activity, (3) Place a fraud alert with a credit bureau.

4. Not all creditors report to all three bureaus, so fraudulent activity might appear on only one report. Checking all three ensures complete visibility of your credit profile.

5. *Common oversights: checking credit reports regularly, using unique passwords for each account, shredding documents, or being careful on social media. Responses should identify why the measure is neglected and potential consequences.*

COMMON MISCONCEPTIONS

Misconception	Clarification
"Identity theft only happens online."	Physical methods like mail theft, dumpster diving, and skimming are still common. Protection requires securing both digital and physical information.
"I'm too young to be a target."	Young people are actually attractive targets because they may not monitor their credit. Some discover theft only when applying for college loans or first jobs.
"A fraud alert and credit freeze are the same."	A fraud alert warns creditors to verify identity but doesn't prevent new accounts. A freeze actually blocks access to your credit report.