

Common types of fraud and scams

Handout 9-7

Telemarketing scams

Telemarketing is the sale of goods or services over the phone. Some telemarketers are annoying, but harmless. Others are selling scams. Signs of telemarketing scams include claims that you have won a prize, such as sweepstakes, travel packages, magazine subscriptions, or gym memberships. Check out the company before you agree to anything. Do not share your credit card or banking information with a telemarketer.

Advance fee scams

These are scams where some kind of service or benefit is offered, but you have to pay before receiving anything. In many cases, you end up paying and getting nothing in return. This is common with guaranteed loans, debt consolidation, and credit repair services. A non-profit credit counsellor will not ask for fees in advance of providing a debt management program.

Debit card fraud

There are many forms of debit card fraud. They all involve stealing your money and banking information. Common scams include:

- Stealing your card and PIN
- Setting up devices to jam your card in ATMs
- “Skimming” which means using a device that can find out your banking information through the magnetic strip on your card
- Fake ATMs that collect your card and PIN information.

For some kinds of debit card fraud, your bank will not cover the money stolen. For example, they will not cover the money if they think that you did not protect your PIN as you should. Make sure that you keep your banking information and PIN secret. Do not share this information with anyone.

Common types of fraud and scams

Handout 9-7 (continued)

Investments fraud and scams

Cryptocurrency fraud

Cryptocurrency frauds involve the use of ads on social media to attract people to invest in cryptocurrency. The ads guarantee high returns, such as 300% growth. The scammers create fake crypto trading platforms and websites. When individuals try to withdraw their money, they realize they have been scammed when they can't reach anyone.

Affinity fraud

Fraudsters approach people through groups such as religious groups, ethnic groups or workforce communities. They gain the trust of the group, then convince people to invest in their schemes. Ponzi or pyramid schemes often work this way. Individuals who join early receive high returns which are paid from other investors' money, but when people stop joining the pyramid, there are no more payouts. This is when people realize they have been scammed.

Foreign scams

You receive a letter or email that claims to be an investment opportunity. The opportunity appears to be from a politician or business leader seeking your banking information so they can share money with you. The scammers then use this information to steal from you or open credit cards under your name.

Boiler room scams

These scams involve setting up a fake office, often called a "boiler room," that has a fake website, a toll-free number, and an address to make the company seem legitimate. By the time you realize the company is fake, you would have lost your invested money, and the scammer will have closed up shop and moved on to another scam.