CONSUMER FRAUD
VII. CREDIT CARD FRAUD SCHEMES

Introduction
Consumers make purchases using credit every day. Credit card companies continuously solicit offers and consumers continue to respond, no matter how unrealistic the perks might seem. This has led to an increase in the number of consumers defrauded by credit card schemes. According to the Nilson Report, close to $22 billion was lost globally to credit card fraud during 2015. It is estimated that by 2020, this number will increase to $31 billion. Credit card fraud can negatively affect the credit of those who become victims. It also increases interest rates and annual fees for all consumers. It is vital that consumers understand of the various types of credit card schemes, so they can reduce their chances of becoming victims.

Credit Card Fraud Schemes
Credit card numbers are frequently stolen at restaurants when servers or clerks processing the bill take a customer’s credit card number for future fraudulent purchases or to sell to other fraudsters. Consumers can also initiate credit card fraud against themselves by responding to fraudulent offers through the mail, by email, or by telephone. When consumers willingly give out their credit card numbers, they are billed for their approved charges, but they also leave themselves vulnerable to additional, unapproved charges. Consumer fraud schemes that involve credit cards include the following:

- Credit card offers
- Secured and unsecured cards
- Gold and platinum cards
- Credit card loss protection plans
- Debit card payments to cab drivers
- Credit card validation codes
- Chip cards
- Credit card interest rate reductions
Credit Card Offers
Individuals receive misleading credit card offers daily. Some advertisements ask consumers to call a toll-free number or visit a website. If the consumer responds, they receive an offer of a Visa or MasterCard and a line of credit. An advance fee is required, either with a bank account number for an unsigned bank draft or through another credit card for the credit product.

Rather than receiving the promised credit card, individuals receive a catalog and an application for a major credit card. Consumers have to purchase a minimum amount of merchandise from the catalog (to build up credit) before they can submit the credit card application. The interest rate on the line of credit is generally extremely high, and the card often can only be used at certain stores or for purchases through other specified mail-order vendors.

Secured and Unsecured Cards
Some companies mislead consumers with advertisements offering credit cards if consumers call a pay-per-call phone number. When individuals call, they are billed for the expensive call. These advertisements promote secured credit cards, which require a savings balance as security for the line of credit. This is not a requirement of standard (unsecured) credit cards.

Secured cards usually charge higher interest rates, have annual fees, and have costly application and processing fees that can total hundreds of dollars. The line of credit for the secured card is usually a percentage of the savings balance. Secured cards are a method of establishing or reestablishing credit, but consumers should be aware of the drawbacks and not misled by the costs.

Advertisements promote “major” unsecured credit cards “regardless of your credit history.” The promotion might claim that cards are issued by an offshore bank, and that no one is turned down. These offers are scams that begin with an advance fee and a promise of a credit card with a high credit limit.

Gold and Platinum Cards
Gold and platinum cards sound like general, all-purpose unsecured credit cards; however, some gold and platinum card offers are disguised solicitations for secured credit cards and are subject to the same scams described in the previous section. Gold and platinum card schemes promise high credit limits with interest-free financing even for those with poor credit histories.

Gold and platinum cards attract customers with promotional offers of “pre-approval with a large credit limit” or “reestablish your good credit.” These scam artists target consumers with poor credit histories.
and falsely claim the cards can improve their credit. Victims believe they will receive an unsecured credit card with full service; however, they soon discover that they can only make purchases from one merchant.

**Credit Card Loss Protection Plans**

Some promoters of credit card loss protection plans misrepresent themselves as representatives of the consumer’s credit card company. They claim that the consumer must have credit card protection to guarantee that criminals cannot access the credit card number online. The purpose of these scams is to obtain a credit card number. These fraudulent companies use additional tactics, such as posing as a representative of a credit card company and asking the consumer to verify their credit card number and expiration date.

Fraudulent companies tell consumers that credit card protection insurance is a certain price. However, after obtaining the credit card information, these companies charge three times the quoted price for the protection. When customers try to cancel, they encounter busy phone lines, excuses, and delays—which makes cancellation virtually impossible.

**Debit Card Payments to Cab Drivers**

More and more cab drivers allow passengers to pay their fare with debit cards. Unfortunately, some have taken advantage of this payment method and devised schemes to defraud passengers. A cab driver initiates a debit card scheme when the passenger arrives at the destination. The cab driver instructs the passenger to enter their PIN on a PIN-pad device after swiping their debit card.

What the passenger does not know is the PIN-pad device captures the PIN along with the passenger’s debit card information. The cab driver has a few uses for this information. He might sell the information to another party or use it to commit other fraud schemes, such as identity theft.

In a variation of this scheme, the passenger arrives at the destination and hands a debit card to the cab driver to pay the fare. The cab driver swipes the card using a legitimate debit card machine—with a card skimmer attached—and waits for the passenger to enter the PIN. Once the PIN is entered, the cab driver hands the passenger a card. The returned card, however, is not the passenger’s card; it is a fake.

The cab driver hopes the passenger will not look at the card before getting out of the cab. When they drive away, the cab driver has the passenger’s PIN and debit card. In this scheme, cab drivers intentionally use poor lighting and choose their victims carefully—usually targeting individuals who
Credit Card Fraud Schemes

seem inebriated and might not discover they have been scammed until the next morning or even a few days later.

The following are tips for consumers to avoid being scammed by a cab driver when using their debit cards as payment:

- Pay cab fares with cash if possible.
- If a debit card must be used, watch every move the cab driver makes when they have possession of the card.
- When a consumer receives the card back, they should make sure it is their card.
- Always ask for a receipt. If the cab driver does not provide a receipt when asked, this is cause for suspicion.

Credit Card Validation Code Scam

There are many variations of the credit card validation scam, but the most common begins with a phone call. The caller gives their name and says they are calling from the fraud department of the credit card company with which the consumer has an account. They tell the consumer that their card has been flagged for an unusual pattern in purchases and they are calling to verify if the purchases are legitimate.

The caller asks the consumer if they purchased an item from a certain merchant for a specific dollar amount. If the consumer says no, the caller tells them that a credit will be issued to their account and all they need is the three-digit validation code on the back of the credit card to verify that the consumer is still in possession of the card. Since the scammer already has their credit card account number, cardholders assume the caller is legitimate; they provide the caller with their three-digit validation code.

Consumers are usually caught off guard because the caller already knows their credit card number; they feel comfortable providing their three-digit validation code. Credit card numbers are not hard for scammers to get, but the three-digit code is. Once the scammers have the code, they are able to make purchases online.

If a consumer receives a call from someone claiming to be from their credit card company who asks for their three-digit validation code, they should immediately hang up. The credit card company already knows the code. If a consumer unknowingly provides their code to a fraudster and later notices unauthorized charges on their account, they should immediately file a fraud report with law enforcement.
Chip Card Scam
Traditional credit cards with magnetic strips are being replaced by Europay, MasterCard, and Visa (EMV) cards, also called chip cards. The purpose of chip cards is to add an extra layer of security against fraudulent point-of-sale transactions by generating unique data for each transaction completed by a consumer. This makes it harder for fraudsters to collect or copy credit card information; however, the risk of credit card fraud remains the same for online transactions, since the EMV technology does not apply to online activity.

As credit card merchants increase security for credit card transactions, such as the chip card technology, fraudsters find ways to skirt these security measures. For example, online scammers send out fraudulent emails to consumers claiming to be from credit card companies. To receive their upgraded chip card, consumers must update their personal information by clicking on a link provided in the email. After clicking the link, malware downloads on their computer. These consumers have unknowingly provided scammers access to information on their computer, which can be used to commit identity theft.

Chip cards have reduced credit card fraud involving card skimmers and other devices used to physically capture credit card numbers. However, schemes that do not require a card to be physically present for the transaction have increased. For example, hackers have increased their activity by hacking into consumer accounts online. Once the scammers have access to credit card information, they open new credit card accounts or sell the information on the black market.

Consumers can protect themselves from chip card scams by doing the following:
- Never give out credit card information via email. Card issuers do not contact consumers before sending new chip cards.
- Contact the credit card company if they receive an email requesting confirmation of personal information.
- Never click on links in emails sent from unknown sources.
- Monitor credit card activity regularly.
- Ensure website URLs contain “https”—the “s” stands for secure—prior to entering credit card information.

Credit Card Interest Rate Reduction Scam
Prerecorded phone calls from agents claiming to be able to lower credit card interest rates for a fee are regularly made to consumers. Consumers should be skeptical and exercise caution because many of them are scams. The companies behind these scams claim to have a special arrangement with the credit card companies. They claim that the lower interest rates are only available for a short time, so consumers
must act fast. Some might even guarantee consumers their money back to entice them to pay for these services.

Consumers can perform these services for themselves for free. Scammers have as much clout as the consumer when it comes to the credit card company and are likely to receive the same outcome, regardless who tries to negotiate a lower interest rate. Victims who pay a fee for this type of scam do not get the services promised, such as lower interest rates, their debt is not paid off faster, and they do not get a refund based on the money-back guarantee.

Consumers who want to lower their interest rate should contact their credit card company directly and not pay a fee to a service provider. There is no fee for contacting a credit card company about lowering the interest rate. If consumers receive calls about lowering their interest for a fee, they should hang up. Consumers should be skeptical of any prerecorded calls.
Review Questions

1. Which of the following is an example of a credit card fraud scheme?
   A. Secured and unsecured card scheme
   B. Debt relief scheme
   C. Consumer debt scheme
   D. Fraudulent loan scheme

2. An __________________________ is an example of a credit card fraud scheme.
   A. Balloon payment scheme
   B. Equity skimming scheme
   C. Credit card interest rate reduction scheme
   D. Credit card debt-collection agency scheme