FINANCIAL SERVICES & IDENTITY FRAUD

SEMINAR PRESENTERS:

MARTHA JOHNSTON, DIRECTOR OF EDUCATION
FINANCE AUTHORITY OF MAINE
Introductions

- Name
- Teaching responsibilities
Seminar Topics

- Financial Services
- Identity Fraud
Financial Services

- Compare & contrast financial services/products
  - Types of financial service providers
  - Services offered by financial institutions
  - Traditional, online, & mobile banking services/features
  - Costs & fees related to financial services
  - Future Banking Trends
  - Un-Banked
Activity

- Earliest “bank” memory

- What do you hope to take away from the financial services session?
  - For your students?
  - For yourself?
Types of Financial Service Providers

- Commercial Banks
- Credit Unions
- Credit Card Companies
- Insurance Companies
- Consumer Finance Companies
- Stock Brokerage & Investment Firms
A commercial bank is a financial institution that provides various financial services, such as accepting deposits and issuing loans.

Commercial banks make money by using their customers' deposits for loans with interest rates above the rates they pay to depositors.
Commercial Banks

- **Deposit Accounts**
  - Checking (Demand Deposit Account), Savings, Certificates of Deposit
  - Most banks offer deposit insurance through the Federal Deposit Insurance Corporation (FDIC)
  - Monthly service fees that are often waived by keeping a minimum balance. Other fees for overdrafts or returned checks.

- **Installment Loans**
  - Secured Loans: Home Loans (Mortgage) & Vehicle Loans (Car, recreational boats)
  - Unsecured Loans: Education Loans & Personal Loans
  - Origination, insurance and/or late payment fees
Credit Unions

Credit unions are an alternative to regular commercial banks and are almost always organized as not-for-profit cooperatives.

Deposits are referred to as “shares”

Unlike commercial banks, access to credit union services is restricted to a particular membership group.

For example; employees of certain companies, members of certain churches, etc.

In recent years, though, membership restrictions have been eased considerably
Credit Unions – Services

- Similar services as commercial banks
- Credit unions typically offer higher rates on deposits and charge lower rates on loans in comparison to commercial banks
- Typically lower fees than commercial banks
- Regulated by different oversight body than a bank and in different ways
- Most credit unions have insurance for their members’ shares available through the National Credit Union Insurance Fund (NCUIF)
Credit Cards

- A credit card is a card issued by a financial company giving the holder an option to borrow funds, usually at point of sale.

- Credit cards charge interest and are primarily used for short-term financing.

- Interest usually begins one month after a purchase is made, and borrowing limits are pre-set according to the individual's credit rating.

- Credit cards can be issued by a credit card company, a commercial bank or a credit union

- Fees – Annualized Percentage Rate (APR) & late payment fees
Insurance Companies

- **Insurance** is a contract, represented by a policy, in which an individual or entity receives financial protection or reimbursement against losses from an insurance company.

- The company pools clients' risks to make payments more affordable for the insured.

- Types: home owners, life, vehicle, renters, malpractice, business, health, etc.
Consumer Finance Companies

- A non-bank lender

- A consumer finance company does not receive deposits, but does make loans to customers for business or personal use

- It derives its profits from the interest on these loans

- A consumer **finance company** generally charges a higher interest rates than a bank
Brokerage Firms & Investment Banks

- Stocker brokerages are firms who buy and sell stocks and other securities for individuals and/or institutional clients through a stock exchange in return for a fee or commission.

- Investment Banks assist in large, complicated financial transactions – for example:
  - Advise on how much a company is worth and how best to structure a deal if the investment banker’s client is considering an acquisition, merger or sale.
  - Issuance of securities as a means of raising money for the client groups, and creating the documentation for the Securities and Exchange Commission necessary for a company to go public.
Types of Banking – Traditional

- Physical locations
  - Bricks & Mortar
  - Branches/Centers
  - ATMs

- Benefits
  - In-person assistance
  - Immediate access to currency
  - Personal relationship

- Drawbacks
  - Inconvenience/accessibility
  - Expensive for banks to maintain
  - Higher fees

- Trends
  - Fewer branches
  - Variety of services & products in one location (financial center); deposits, withdrawals, loans, mortgages, payment processing, financial advising, business banking
Types of Banking – Online

- **Internet-based**
  - Online option through traditional bank
  - Online bank with no physical branches

- **Benefits**
  - Account access & transactions conducted anytime from anywhere
  - Online loan applications
  - Lower fees

- **Drawbacks**
  - No in-person assistance
  - No personal relationship
  - No access to currency
  - Some transactions are time constrained
  - Technology dependent
  - Cybersecurity

- **Trends**
  - Increasing usage
  - Increasing options
  - Partnering, e.g. Mint
Types of Banking – Mobile

- Internet-based App
  - Offered by any type of bank
  - Phone or tablet usage

- Benefits
  - Digital wallet
  - Text alerts
  - Most accounts can be accessed & transactions conducted anytime from anywhere
  - Remote deposit
  - Online loan applications

- Drawbacks
  - No access to currency
  - Inconvenient for loan applications
  - App may limit which accounts can be accessed
  - Technology dependent
  - Cybersecurity

- Trends
  - Attracts younger customers
  - Compatible with digital wallets e.g. Venmo
Future Banking Trends — 7 New Technologies in Next 5 Years

- Blockchain Technology (think BitCoin)
- Upgraded ATMs (biometric authentication)
- Growth of Non-Banks
- Apple Store-style Experience (customer issues/concierge service)
- Automated Financial Services Employees (robo-advisors)
- Mobile & Digital Banking (we’re on the tip of the iceberg)
- Strategic partnerships (data informs all)

Source: https://www.gobankingrates.com/banking/6-banking-technologies-youll-see-next-5-years/
Banks and Credits Unions
The “Un-Banked”

- Don’t think they have enough money to open an account
- Lack understanding about US banking system & expectations for having a bank account
- Have past negative banking experience in the United States
- Have had negative banking experiences in their homeland (i.e., banks not insured)
- Lack appropriate documentation needed to open a bank account
- Fear being "reported" to authorities (i.e., illegal immigrants, in hiding)
- Have an unstable living situation
- Have cultural conflicts including bank practices that vary with personal beliefs
The Cost of Being Un-Banked

Source: https://www.nerdwallet.com/blog/banking/unbanked-consumer-study/
Classroom Resources

- Money Smart by Federal Deposit Insurance Company (FDIC)

- Next Gen Personal Finance
  - http://nextgenpersonalfinance.org/
Think about how you can integrate what you have learned into your own life and into your classroom instruction.

One thing you learned that you hadn’t realized before today that you will use managing your own money.

One thing that you plan to explore, use, develop for your students.
15 Minute Break
Identity Fraud

- Identity theft, fraud and scams
  - Identity theft and fraud statistics
  - Financial impact of fraud
    - Individuals
    - Society
  - How identity information is stolen & deceptively used
  - Ways to protect against identify fraud
Identity Fraud – Knowledge is Power

- It’s all about the money
  - People are working hard to steal your money
    ... it’s their occupation, and they’re good at it

- Assuming it won’t happen to you won’t make it go away
  - The best offense is a good defense

- Be informed
  - Minimize the damage should this happens to you
Maine & Identity Fraud

- **2016 Federal Trade Commission – Maine is:**
  - # 29 – Identity Theft Complaints
    - Number one is Michigan
    - Number two is Florida
  - # 41 – Fraud and Other Complaints
    - Number one Florida
    - Number two is Georgia
What are the Scams?

Take the next 6 minutes to brainstorm the top ten scams.
Impact of Identity Theft

**Individuals**
- Financial – loss of assets
- Credit Issues – amassed debt or unknown late payments
- Benefits – using SSN (health or financial)
- Legal – crime committed in your name (rare, but happens)
- Onerous and time consuming to fix

**Society**
- Millions of people impacted and the residual effect on their well-being and ability to participate in economy
Protect Your Mail

- Get it out of the mailbox ASAP
  - Bad people go through your mail

- Shred, Shred, Shred
  - Buy a cross-cut shredder
  - Shred everything with personal information on it

- Do not send mail using your home mailbox
  - Best – use the U.S. Post Office and go inside
  - Next Best – use the blue mailbox – but, not always safe

- Online documents are the way to go
Protect Your Property

- Home and garage
  - Lock doors and windows . . . especially door from garage to house
  - Secure important documents

- Car
  - Lock doors; roll up windows
  - If you want it stolen, leave it in your car
  - Don’t leave your car running & unattended
Computer Fraud (part 1)

- Basics
  - Know how to operate your computer
  - Install the latest anti-virus & spyware software
    - Run software; ensure you’re getting updates
  - Ensure system & browser software are up-to-date
  - Install firewall (either hardware or software)
  - Protect wireless system
    - Mask the name of the router (DO NOT USE...Smith’s router, 12345 West St., etc.)
    - Use strong password
Passwords (all computer applications)

- Use strong passwords
  - > 8 completely random numbers, letters, and special characters (use all of the types that are allowed)

- Do not store passwords online or on the computer
  - Write them down and keep them secure

- Do not reveal passwords to anyone

- Do not use the “save my password” feature for applications and websites
Enjoy E-mails, but be careful

- Things are not always what they seem to be
  - Don’t believe everything you see and read

- Scams, viruses, and worse . . . oh my
  - They want you to **wire** money
  - Look at the cute puppy . . . bad stuff embedded in pictures
  - *There’s a problem with your account, confirm your password, date of birth, SSN, etc.*
  - **Click on this link to . . .**
E-mails (continued)

- Be weary of all e-mails
  - They may not have been sent by whom you think
  - Access the website independently, not through the link
  - Never, never, never provide personal information to anyone, unless you initiate the contact with a known entity
Computer Fraud (part 5)

- Again – firewalls, antivirus and spyware software are important
  - Viruses
  - Trojans
  - Bots

  - When hackers take over your computer to do a dastardly deed
  - What do you do when the police knock on your door?
Banking Fraud
(part 1)

- Be proactive
  - Check all of your accounts; check them often

- Passwords
  - Set up every online password that’s possible
    - Don’t leave accounts with a “password” password
    - If you’re not going to access it online, contact the bank and have them deactivate it
Passwords (continued)

- Use very strong passwords (letters, numbers, special characters, and length)
- Change them at least every six months

Accessing sites

- Do not click on the links found in documents
- Access the sites independently
Revealing information to your bank

- The bank knows all of your passwords, account numbers, and personal information.

- If you receive a call from your “bank” and they want you to provide information to confirm it’s you, **don’t do it**.
  - Take down their name, number, department, etc.; use a known number to contact the bank.

- However, your bank will generally call if there’s suspicious activity on your credit card.
  - Be proactive – check and check often.
Banking Fraud (part 4)

- **Statements**
  - Sign up for electronic statements
    - Eliminates need to shred paper
    - Less mail for you

- **Pay bills electronically**
  - Stop writing checks – set up online payments
    - Push from your bank or pull from the business
    - Easy, convenient, and you save on the expense of checks and stamps
Banking Fraud (part 5)

- Direct Deposit
  - Use it, don’t get paid by check

- Checks
  - Use electronic payments whenever possible
  - Be careful who you give a check to
  - Don’t put your SSN or date of birth on a check
Protect Credit, Charge, Debit Cards

- **Credit & Charge cards** — loans from card companies
  - Fair Credit Billing Act — liable up to $50 for fraudulent purchases (unauthorized charges)
  - It all depends on your card company

- **Debit card** — money withdrawn from your account
  - Electronic Transfer Act — if bank is notified within 2 days of you learning about the fraud, your liability is limited to $50
    - Two to six days, your liability is limited to $500
  - It all depends on your bank’s policies
Protect Credit, Charge, Debit Cards

- **RFID** – chips in the cards
  - Card info can be read from a distance

- **ATM machines**
  - Skimmers and cameras attached to the ATM

- **Gas Stations**
  - Skimmers attached to card readers at the pump
Protect Credit, Charge, Debit Cards

- Set limits on daily Debit card charges
- Set up e-mail and text alerts for bank accounts and credit/charge cards (check with bank & card company)
  - Charges over a certain amount
  - Withdrawals over a certain amount
  - Daily balances
  - Etc.
- Monitor your accounts on a frequent basis
- Set up all passwords . . . make them strong passwords
- Notify your card company when you’re traveling
Protect Credit, Charge, Debit Cards

- Purchase “sleeves” for RFID cards
- Eliminate paper statements
- Cover your hand when you enter your PIN
- When in doubt, pull on the card reader to see if it’s attached
- Look for small cameras
- Shred credit card offers
  - To reduce offers, call 1-888-5-OPTOUT (1-888-567-6868) or enroll online https://www.optoutprescreen.com
- Pay attention to letters from your bank that confirm changes to your account
Medical Fraud

- Always review your Explanation of Benefits (EOB)
  - Did you actually receive the treatment, services, medical equipment, etc.?
  - Check your credit report annually
    - Are there delinquent charges for treatment you’re not aware of?
Protect Your Child’s Identity

- Ripe for identity theft
  - Social Security Numbers
  - Birthdates
  - Etc.

- Familial fraud is most common

- Takes many years to identify

- Possible clues
  - Mail and credit card offers in the child’s name
  - Bill collectors calling regarding the child

- Possible prevention – free annual credit report
Be careful what information you put out there

- Pictures – family, house, pets, etc.
- Birthdates
- Addresses
- Nicknames
- Names of family members, pets, etc.
- When you’re going on vacation
- Other types of personal information

Remember, once it’s out there . . .
- it’s there forever . . .
- nothing ever gets destroyed
Who/What You Can’t Control

- Everyone else
  - Banks
  - Credit card companies
  - Medical offices
  - Internet, etc.

- Don’t be so trusting; don’t be paranoid, **Be Proactive**

- What to do
  - Use common sense
  - Check, and check often
  - You are your best defense
Credit Report

- Get your free annual credit report...
  (https://www.annualcreditreport.com)

- Does not include your credit score . . . you’ll have to pay for this feature

- Review it and compare it to known sources of credit
  - Look for unfamiliar medical claims, loans, names, address, and any other types information

- If there’s fraud
  - Go to any credit bureau to put a fraud alert on your account
  - Report it to the police
  - Contact creditor
The Facts about Fraud

- 9,000,000 Americans have their identities stolen each year

- Every three seconds another identity is stolen in the U.S.

Source: Federal Trade Commission
Activity

What’s In Your Wallet?
Remember . . .

If it sounds too good to be true,

it is!
For More Information

Federal Trade Commission (FTC)
www.ftc.gov/bcp/edu/microsites/idtheft/

Federal Bureau of Investigation (FBI)
fbi.gov

U.S. Department of Justice (DOJ)
www.justice.gov/criminal/fraud/websites/idtheft.html

Internet Crime Complaint Center (IC3)
www.ic3.gov/default.aspx

Identity Theft Task Force
www.idtheft.gov/

[state] Bureau of Investigation
[website]
Reflection
Financial Services

- Think about how you can integrate what you have learned into your own life and into your classroom instruction.

- One thing you learned that you hadn’t realized before today that you will use to protect yourself from identity theft and fraud.

- One thing that you plan to explore, use, develop for your students.