Topic 10: Credit Problems & Financial Scams

Features

- Ubiquity
  - 1 in 3 Americans have a subprime credit rating
  - 25% of Americans have a poor credit rating of under 600
    - 20% under 580
  - Credit fraud is fastest growing crime in US
    - 1.4 million identity theft cases reported to FTC in 2021
    - Phone fraud cost 68.4 million Americans money in 2022
  - Text, email, phone and social-media based frauds

- Sophistication
  - All age groups affected
  - Use of voice prints in AI-based fraud

Topics For Today

- Poor credit rating (bad credit)
- Temporary inability to pay your debts (due to job loss, illness, etc.)
- Drowning in debt (and perhaps getting calls from debt collectors)
- Credit fraud & identify theft
- Identifying and avoiding financial scams

Issue 1: Bad Credit

- Do's
  - Check credit record and remove incorrect negative information
  - Work on improving your credit score
    - Payment history (35%) and utilization rate (30%)
  - Have hope
    - Remember that last two years of your credit history is the most important
    - Key want to avoid adverse credit events (charge offs, collections, and bankruptcy) since these stay on your record for a long time - TBD
  - Contact **non-profit** credit counselor for help

Issue 1: Bad Credit

- Do's
  - Check credit record and remove incorrect negative information
  - Work on improving your credit score
    - Payment history (35%) and utilization rate (30%)
  - Have hope
    - Remember that last two years of your credit history is the most important
    - Key want to avoid adverse credit events (charge offs, collections, and bankruptcy) since these stay on your record for a long time - TBD
  - Contact **non-profit** credit counselor for help

- Don'ts
  - Use firms that offer to fix your credit for a fee
    - Often pay fee for little in return
    - "Credit washing" at best a temporary fix
    - Danger of unscrupulous firms misusing your information (identity theft)
  - Utilize "bad credit/no credit" lending opportunities
    - Very high interest rates
    - Especially want to avoid "pay day" loans - TBD

Issue 2: Temporary Inability Pay Debts

- Examples: Lost job, illness, sudden losses/urgent expenses

- Need: Credit forbearance
  - Temporary postponement or reduction in debt payments
  - Avoidance of charge offs, debt sent to collection, etc.

- Availability
  - Federal student loans
    - Can apply to defer payments for up to three years
  - Private student loans
    - Typically can only defer payments for 1 year
  - Other: case-by-case but worth trying
    - Can approach banks and other lenders
      - See Kobliner on getting to know your banker, etc.
      - But will want to scrutinize your budget beforehand

Issue 2: Temporary Inability Pay Debts (2)

- Do's
  - Make sure you have scrutinized your budget beforehand
    - Asking for a payment cut on your loans when you are spending $500/month on Netflix and restaurants is not a good look
  - Talk with a nonprofit credit counselor if you want help with budgeting process or how best to approach lenders

- Don'ts
  - Just stop paying without explanation or applying for forbearance
  - Let debts pile up to an unsustainably high level
  - Just pay minimum balance on credit card if you can avoid it.

- Just remember
  - Forbearance is just a temporary solution
  - And monthly debt payments will likely be higher after forbearance period because
    - Interest has been accumulating on unpaid debts
    - Remaining period to pay off loan has lessened

Issue 3: What If You are Drowning in Debt?

- Bad old days
  - Debt slavery
  - Debtor's prison

- What about today?
  - Mississippi?
  - Federal student loans?
  - IRS (US tax) obligations?
  - Other?
    - Lender will need to go to court
      - Mortgages and auto loans
      - Other loans
      - But can still face seizures, debt collectors, garnishment, etc.

- Goals for today
  - Make sure you know your rights
  - Identify positive ways to go forward
  - Understand what actions you need to avoid

Handling of Delinquencies

- Federal Student Loans
  - Enter default 270 days after nonpayment
  - After that, usually have options to restore your good credit standing

- Private Loans
  - Typically enter default after 30 days on nonpayment
  - May be charged off in as little as 120 days of nonpayment
  - Very limited options to get out of default after it is charged off

What If You Are In Default? (No Liens)

- Federal Student Loans
  - Debt collectors can bypass courts and directly seize your tax refund or garnish your wages
  - And then can do this indefinitely (*even your social security*)!!!
    - (*That is, federal student debt is generally **NOT** wiped out by bankruptcy*)
    - In other words, you can't get out of this debt
    - So make sure you can afford to carry this debt.

- Private Loans
  - Rely on court system to sue and collect a judgment
  - And are subject to your state's statue of limitations
  - But you still really want to avoid living through this
    - One issue: Dealing with debt collectors

Dealing With Debt Collectors: Your Rights

- The debt collector business model
  - And the bad old days

- Debt collectors today
  - Can contact you via phone, fax, email, & in person, but only during reasonable hours (e.g. 8AM – 9PM)
  - They can't harass you. Can't call you at work if you say your boss does not allow it, and they can't tell your boss about it.

- But you want to avoid it coming to this
  - So what can you do before the loan is charged off?
  - Goal: Getting payments to a level you can afford
    - Possible approaches: Maturity extension, interest rate cut, partial principal forgiveness

Things To Do When You Have Debt Problems

- Talk to your lenders and explain situation
  - They will likely prefer working something out to the alternative (*debt collection, foreclosure, or bankruptcy*).
  - But note reasons why they may not be able/willing to help
    - Loan was securitized, signaling problem, poor presentation on your part

- Think about contacting a **nonprofit** credit counsellor
  - Can get advice on budgeting, your rights, and best way forward
  - I think that can help your presentation to lender, while Kobliner reverses the order.

- Avoid pressure to make fast decisions
  - The dual challenge of money and time scarcity
  - And the problems of “tunnelling” when faced with scarcity

Things NOT To Do When You Have Debt Problems

- Use a fee-based service that promises to repair your debt problem
  - Often pay fee for little help.
  - May even expose you to identify theft if service is sufficiently unscrupulous

- Use payday lenders
  - Loans are small (often <$500) and only last for a couple of weeks
    - You write a check dated on day you get paid (they will want to see your paystub)
    - And they they will charge you a fee for the service
  - Problem: huge interest rates implied by those fees
    - Implied APR on $100 loan for 2 weeks with $15 fee is 390% (CA max is 480%)
    - Effective interest rate on this loan is 3,686%
    - Won't get out of this debt if it is allowed to grow

What About Bankruptcy?

- Can get many debts (*credit card, landlord, doctor*) discharged
- But can still face foreclosure and remember that student loans – are not discharged.
  - Instead federal debt servicers can garnish your salary and take your tax refund
- Potential employers will be able to see your bankruptcy on your credit record
  - Which can make it hard to change jobs.
- And this will be on your record for a long time – at least 10 years
- In other words, a last resort
  - And consequences of a bankruptcy can be more severe outside the US

Issue 4: Credit Card Fraud & Identity Theft

- Fastest growing crime in the US
  - Version 1: Run credit card charges, debit card & other payments in your name
  - Version 2: Access your financial accounts to make payments; take out loans in your name; even clean out your asset accounts

- Will happen to you (*at least in a mild way*)

- Will want to protect yourself
  - From identity theft
  - And be able to limit consequences of identity theft

A First Scenario

Suppose someone starts making charges using your credit card number, debit card number, Zelle, Venmo or other payment systems

Issue: How much fraud protection do you get?

- US Credit card:
  - US law limits your risk to $50 (*and this is often forgiven*)
  - So expect them to monitor charges carefully, and deny
    - Unusual charges (esp. large charges)
    - International charges
    - So let them know before you plan to travel or make a large/unusual purchase
  - In case of fraud, they will cancel old card and send you a new one
  - Still should be checking your monthly statement for unexpected charges
  - *Note – responsibility for identity theft can differ with cards from other countries*

How Much Fraud Protection Do You Get? - 2

- US Debit Card
  - Loss protection is less clear cut
    - Loss limited to $50 if you report problem within 48 hours of start of abuse
    - Loss limit then rises to $500
    - And is unlimited if you take 60 days or more to report problem
  - So you are at risk if you are not daily monitoring your charges online

Note: Fraud protection can be much less with nonUS credit and debit cards

- Paypal, Zelle, Venmo, etc.
  - Paypal has some legal protections
  - Zelle, Venmo, etc. do not

- Bank wires
  - Money is essentially gone after it is wired

Two Things To Watch Out For

- Card readers at gas pumps, etc.

- “Glue and tap” fraud at ATMs
  - Fraudster jams ATM card slot
  - Then suggests you can bypass slot using “tap” function
  - Scammer can access your account if you don’t log out

Some Rules For Using Credit/Debit Cards

Implications, Why I:

- Use my credit card instead of my debit card to make purchases
  - And only use my debit card to withdraw money from my own bank's ATMS.
- Make sure I have back-up (*no fee*) credit cards
- Advise credit card company before travelling or making large or unusual purchases
- Never use my credit or debit cards at gas pumps or other places where scammers often install card readers.
- Often used some US credit cards instead of my UK cards when living in the UK
  - But only after making sure the US cards were on automatic direct debit
  - And had thoroughly checked out the FX fees.

A Scarier Scenario

You start getting calls from debt collectors about loans you never took out.

Implications:

- Federal law often, but not always, protects you from fraudulent charges
- But your credit score & report has been ruined, likely for a long time
- And it will take a long time to restore your identity

Prevention

- Check credit card and bank balances regularly
- Pick up mail every day
- Shred all bank statements, accounts, tax records, etc.
- Never give personal information on phone or internet
  - Street address, birthdate, Social Security #, email, phone number, account numbers, etc.
- Be super sensitive about potential scammers (like text & phone messages)
  - I only reply by using the numbers at the back of my credit card, etc. (not the one they give me in the text – only have one exception)
  - *Note how I got sucked in by a fake email from a Pitzer dean*
- Check credit reports fairly regularly
  - Kobliner: Value of monitoring services less clear if you are being careful

A Scarier Scenario - 2

You start getting calls from debt collectors about loans you never took out.

What if you detect/fear identity theft?

- Key: Stop additional loan creation by thieves
  By stopping requests when they reach the credit bureau

- Simplest strategy: Call each credit bureau and set up a fraud alert
  - Basically a written warning on your credit report that your identity has been stolen.
  - Good for 90 days

- Stronger strategy: Create an extended fraud alert.
  - Go to IdentityTheft.gov and create an Identity Theft Victim's Affidavit and Complaint
  - Take it in person to your local police station and fill out an official police report
  - Provide each credit bureau with copies of affidavit and police report and have them place an Extended Fraud Alert
  - Good for 7 years

A Scarier Scenario - 3

You start getting calls from debt collectors about loans you never took out.

What if you detect/fear identity theft?

- Strongest strategy: Place a credit freeze with each credit bureau
  - Generally costs $10 each
  - Now only people who already have a credit relationship with you can see your report
  - You will need to use a customized PIN code to “unthaw” freeze if you need to apply for credit (so don’t lose that PIN)
    - Will also need to unthaw freeze when applying for utilities, etc. that check your credit before allowing an account.

A Final Scenario

Are you sure no one can access your bank, fund and brokerage accounts and clean you out?

- Remember, most of us access our accounts via the internet

- Prevention Strategy #1: Use super strong passwords
  - Which you change regularly
  - And don't store in places that are easy to access
  - Issue: what about password devices?

- Prevention Strategy #2: Two-step verification
  - Yes it's a pain but do you really want the firms holding your assets to remember your laptop?

- Prevention Strategy #3: Don't do your finances over public wifi

Issue 5: Financial Scams

Lead article in August 2023 Consumer Reports

- Growing role of technology in our lives
  - Importance of phone, email, text, social media etc.
  - Problem: but also key vehicles for criminals to take advantage of us (scams)
  - Goals: Money & Information (Identity)
    - Access to your assets
    - Create loans
    - Trick your associates into providing their information

- Why do we get scammed?
  - Behavioral biases: *including extrapolation, truth bias, & tunneling (if under pressure)*
  - Fortunately believable timing (2 examples; email to me, bank alert)
  - Sophistication (AI voice prints)

- Issues:
  - Awareness
  - Strategies to avoid scams
  - What to do if you get tricked (*reveal info, click that tab*)

Text Scams (Smishing)

- Now 22% of all fraud reports to FTC
  - Starting to overtake phone fraud (or phishing)

- You know the drill
  - Problems with your Netflix, Amazon, etc. account
  - Suspicious/fraudulent activity detected with your credit card, bank account, etc.
  - Won a prize or due a refund
  - Prescription drugs or other item for sale
  - Seeking support for political group, charity, etc.
  - *Just click on the link!*

- Typical goals
  - 60% of scam texts will implement malware on your device
  - Rest take to a web page to get info, such as
    - Netflix account number
    - Credit card numbers to pay for goods, or shipping & taxes on free prize

Text Scams (Smishing) - 2

- Note:
  - Opening text or sending simple reply will not put you in danger of malware
  - But replying will tell them the number is active – and lead to more texts

- Don’ts
  - Click links
  - Click “unsubscribe” or “stop” links
  - Call the number they recommend

- Do’s
  - Look up and call bank or credit card number (like the one on the back of your card) to see if there is a problem
  - Talk with fraud department at that institution if believe the account may have been compromised
    - Immediately change passwords and usernames on those accounts
    - Delete URL from browsing history
    - And take device to tech repair service (especially if it does not work)

Phone Scams (Phishing)

- Examples
  - Owe money or in line for a refund from a company
  - Owe money to US (fake IRS call)
  - Problems with social security payment
  - And all pressing you to act quickly

- Basic rules
  - Let unsolicited calls (not from someone on your call list) go to voice mail
    - Doesn’t tell them it is a live number and the fakes hang up
    - Picking up phone tells them it is a live number, which increases future calls
  - Don’t get on phone just to drive phisher crazy
    - Remember, one goal may be to get your voice print for other scams
    - Alternative of AI-based programs to drive phishers crazy
  - If you think message may be genuine
    - Look up and call bank, IRS, etc. if not sure (like the number on my credit card)
  - Have a safety word with family members to identify them
    - Or just call them back

Email Scams

- Examples
  - Which are getting more realistic with Chat GPT, etc.
  - Usually ask you to click link to update credentials
  - In my case scammer was looking for my phone contacts

Basic rules

- Without opening email, let cursor hover over sender's name
  - Will bring up the full address
- Remember businesses and IRS usually won't be asking you to click a link
  - Instead they usually ask you to log into your account with them
- Check out CharityNavigator.org to get information on how the charity is rated (assuming it is a real charity)
- Note: You are OK if you open an email but did not click a link or download an attachment

Social Media Scams

- Starting point for 11% of scams in 2022
  - Ads for bargains, Low-interest loans, Crypto investments etc.
  - Friend requests from strangers (or from people who claim to know someone you know)
    - Issue: friend or family member may have already been hacked

- Danger
  - Not from messaging
  - But from giving people access to personal info on your social media pages that can be used for identity theft, such as determining answers to security questions on your other accounts

- Good practice
  - Not friending someone until you have checked them out directly (with shared person)
  - Limiting personal information on your social media pages

Some Smart Security Steps

First seven from lead article in August 2023 Consumer Reports

- Slow down
  - Beware of demands for immediate action
- Share less of your personal information
  - Both in revealing your favorite musician on social media
  - And in taking their endless quizzes
- Delete old accounts
- Allow automatic software updates
- Two-Step Verification
- Stick with safe payment methods (credit card vs. Venmo)
- Antivirus protection
- *And from me – contact business, etc. directly instead of using numbers, links in texts, etc.*