Preventing ID Theft: Information from Slides

The Purpose of ID Theft

- Utilizing your existing accounts (Credit Card / Bank) ▪ This can be simple spending or complex like changing addresses
- Open New accounts ▪ Credit Cards, Bank Accounts, Loans, Utility Accounts
- File for your tax refund
- Get medical care / Insurance coverage
- For purposes of employment or arrest

Limiting Exposure

- Adopt a “Need to Know” approach with regard to Personal Information
- Store all Personal Information in a secure location
- Carry only necessary cards and identification (Limit what’s in your wallet)
- Know what personal information is online and what information you are sharing
- Utilize unique strong passwords for each separate account
- Only shop on trusted secured websites ”https://” 🔒
- Protect your mail; Prior to and after pickup
- Never sign up for “Free” Offers and be leery of organizations / clubs
- Install security software on computer and be aware of scams
- Pay attention to bills and statements
- Check your credit at least once a year
- Never write PINS or passwords down
- Monitor CCs and receipts when purchasing in person
- Guard your SSN; very few transactions actually need this number
- Shield your PINs and passwords from others
- Never give out your PINs or passwords
- Sign your CCs immediately when you receive them
- Only utilize secure Internet sources for access to data with passwords
- Sign up for the Federal Do Not Call List Donotcall.gov
- Sign up for Opting out of preapproved CCs Opoutprescreen.com
- Never utilize RFID cards; elect for EMV cards
- Always communicate with financial institutions by initiating contact
- Used 2 Factor Authentication on any available account
- Set up notification alerts on your financial accounts

What to look for

- Unknown charges on accounts
- Statements show up for unknown accounts
- Errors on your credit report
- Contacted by a financial institution or creditors
- Missing mail or normal bills
- Denied credit

Preventing ID Theft: Information from Slides

If you are a victim

1. Call the companies where the theft, fraud or ID theft occurred
   - Call the company whose account was compromised
     - Explain to the fraud department that your identity was stolen.
     - Document the conversation
   - Ask the company to freeze and/or close the account
     - Then there can be no additional charges
   - Change all logins, passwords and PINs.
2. Place Fraud Alert or Freeze on your Credit
   - Contact the credit bureaus
     - Nothing less than a free 90 Fraud Alert
     - Experian – 1-888-397-3742
     - Equifax – 1-888-766-0008
     - TransUnion – 1-800-680-7289
   - Consider Freezing credit or an Extended Fraud Alert
     - Alerts will be passed on between bureaus, Freezes will not
     - Freezes cost typically $10 to enact and disable, Alerts are free
   - Request a credit report – www.annualcreditreport.com.
3. Report ID Theft online to Federal Trade Commission
   - www.identitytheft.gov
     - Online forms or call 1-877-438-4338
     - Recovery steps, Reporting, and Resources
   - Creating an account
     - Walk through recovery steps, make a plan, track progress, and pre-fill forms
   - Reporting without account
     - Once you complete your report, print and save plan and report because it will not be saved.
4. Make a police report with local law enforcement
   - Contact local law enforcement to file a report
     - Provide as much information about the ID Theft a possible
     - Provide the FTC Identity Theft Report
   - Document the case number
     - Document the Law Enforcement Officer's Name
   - Request a copy of your report
     - After the case is complete you can request a copy at the local office.

Data Breaches

- Consider the free credit monitoring that is offered
- Request your Credit Report
- Consider Freezing your Credit
- File your Taxes Early
- If notified about other account comprise; Contact them

Preventing ID Theft: Information from Slides

Recovery

- The first steps are time sensitive
  - Act fast as this will stop the ”bleeding”!
- The rest is a marathon, not a sprint
  - Keep extensive logs and/or notes
  - Ask for names of people and documentation of communication
  - Send all information certified or document the receipt
  - Document all expenses and participate in the court process
- Reviewing you credit report
  - Compare with known accounts
  - Look for anomalies (i.e. misspellings, wrong name, etc.)
  - If you locate additional compromises, start over with the URGENT steps
- Close New Accounts
  - Contact the fraud department and explain that your identity was stolen
  - Have a copy of your ID Theft report and ID Theft Dispute Letter
    - Sample letters available at www.identitytheft.gov
  - Ask the business for a letter confirming the following:
    - The Fraudulent Account isn’t yours
    - You aren’t liable for the account
    - The account was closed
    - It was removed from your credit
    - Confirming that the Fraudulent Charges were removed
  - Keep the letter for your records
  - Document who you spoke with along with the date and time.
- Correct your Credit Report
  - Draft a ID Theft letter to the Credit Bureaus
    - One for each Bureau; Experian, Equifax, and TransUnion
    - Sample letters available at www.identitytheft.gov
  - Have a copy of your ID Theft report
    - You can do this without a report, but it more streamlined with a report
  - Request to have the fraudulent charges removed from your credit report
    - Make it easy on the Bureaus: Provide the information about the fraudulent accounts in both writing and circled on a credit report.
  - Keep the documents for your records

Resources

- Federal Trade Commission
  - www.ftc.gov
  - www.identitytheft.gov
  - www.consumer.gov
- Oregon DOJ – Consumer Protection
  - www.doj.state.or.us/consumer-protection
  - Trust only known sources
  - Government Sites, Credit Bureaus, Known Monitoring solutions, Banks, Credit Unions