



Important Information about this Presentation

- The views and opinions expressed in this presentation are those of the presenter. They do not necessarily reflect the views or positions of the DFPI.
- This presentation is for educational and informational purposes only. This is not financial or legal advice and does not replace independent or professional judgment.
- The DFPI does not assume responsibility for the completeness of the information presented in this presentation.
- Please feel free to take notes and ask questions during the presentation. But there will be a dedicated time at the end for a live Q&A.
- You can get a copy of these slides by emailing: <u>Outreach@dfpi.ca.gov</u>







The Department of Financial Protection & Innovation

Who Are We? What Is Our Role?

- The DFPI's central purpose is to maintain a fair, healthy, and trusted financial services marketplace for all Californians.
- The Department accomplishes its mission through regulation and enforcement of a variety of financial services, products, and professionals.
- Provide presentations throughout California to inform and protect consumers and to prevent them from falling prey to frauds and scams.
- **Learn more at:** <u>dfpi.ca.gov/consumers</u>

Call us at:

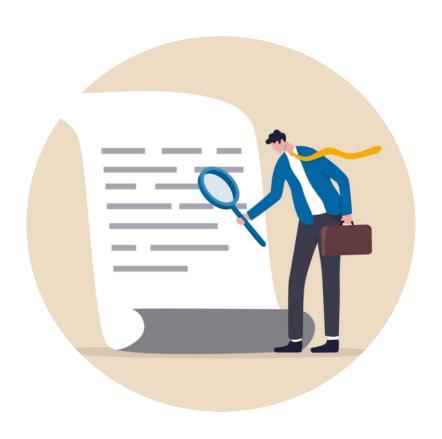
1-800-275-2677





Who Does the DFPI License, Regulate, or Oversee?

- State-chartered banks and credit unions
- Foreign banks
- Broker-dealers and investment advisers
- Payday lenders
- Mortgage lenders and loan originators
- Debt collectors
- Escrow agents
- Franchise investments
- Money transmitters
- Student loan Servicers
- Trust companies
- And more! For a full list, visit: <u>dfpi.ca.gov/licensees-and-regulated-industries</u>





Access Free Online Financial Education

These courses are designed to meet you where you are, help build your money management skills and demystify the world of personal finance.

Course topics include:

- Budgeting
- Investing education
- Retirement planning
- Paying for college
- Debt management
- and more!

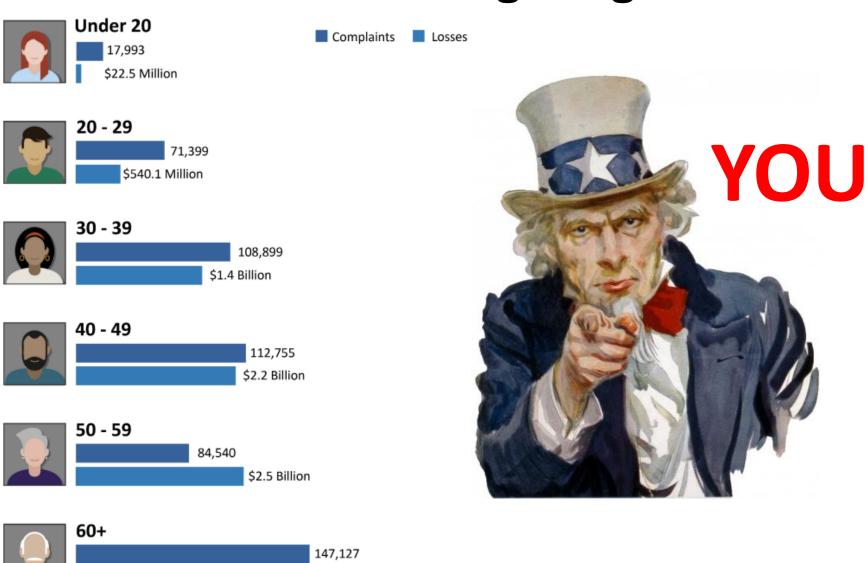




Get started at: dfpi.ca.gov/learn

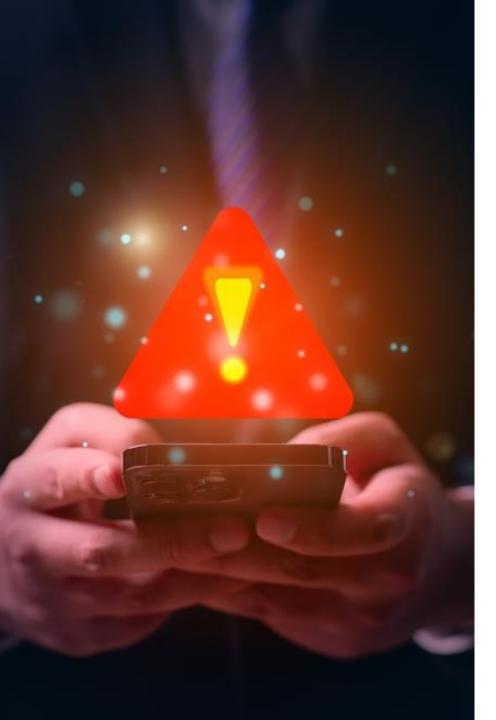


Who Are Scammers Targeting?



\$4.8 Billion





Beware these Common Scams

Imposter Scams

- Grandparent/Relative scams
- Debt collectors
- Government imposters:
 - IRS / Social Security
 - Utility company
 - Law enforcement
 - Financial institutions
- Prize scams
- Investment scams
- Romance scams
- Tech support scams
- Payment app scams
- Student loan scams
- Employment scams





Money Apps / Transfer Scams

BEFORE sending money through an app:

- Always make sure you're sending or accepting money from the correct person.
- You have the physical product or the service has been completed.
- **Do not** accept payment from someone you don't know.
- Do not send money back as a refund or overpayment.

Free Msg-Suncoast Credit
Union Alert-Did You Attempt
A Zelle Payment For The
Amount of \$5000.00?
Reply YES or NO Or 1 To
Decline Fraud Alerts





Website Link Safety



BEFORE you buy online or login to a website:

- 1. Always **CHECK** website *link* to make sure it's legitimate!
- 2. Check to make sure the website connection is secure:



Connection between your web browser and the website server is encrypted



Just like an ID card confirms a person's identity, a private key confirms server identity.



How Can You Protect Yourself?





1. Do Not Respond to Scammers



Ignore <u>anyone</u> contacting you that you don't know.

- ☐ Vishing Telephone
- ☐ Phishing Computer/Emails
- ☐ Smishing Text Messages
 - ☐ "Click here"
 - ☐ "Callback number"
 - ☐ "Reply back"





2. Do Your Research!

- Look for red flags.
- Verify information.
- Check credentials.
- Go <u>directly</u> to the <u>official</u> source, company, or website.
- Get Help: ask an employee or professional in person.



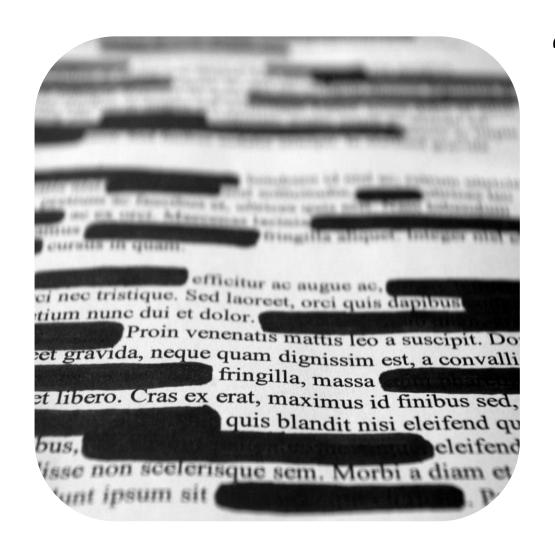
3. Take Your Time

Ignore anyone who is:

- Threatening you
- Giving you a limited-time offer
- Telling you not to share this information with others
- Asking for your personal or financial information
- ✓ Do not make any big financial decisions for at least 24 hours







4. Do Not Share Your Info

Limit what information you share on:

- Social media
- Websites, forums, communities
- Emails
- Sign-up forms
- Online shopping sites
- Phone apps
- Company or account profiles

***When a company suffers a data breach, the more information you've shared, the more you are exposed.



5. Talk Someone You Trust

Another person can provide additional perspective and can often point out red flags that you miss.

Talk to someone and get help from:

- Spouse
- Friend
- Children (18 years or older)
- Community leader
- Financial advisor or professional







6. Stay Vigilant

Regularly check your:

- Financial accounts
- Credit reports
- Delete unused accounts and have your data removed from sites
- Use a shredder to dispose of mail and personal documents
- Deposit important mail directly to the post office
- Don't just close your Internet browser log out of websites
- Use anti-theft gel pens for checks and other signature documents



Don't forget to Report the Incident

Report this scam to:

- Local authorities
 - Police
 - District attorney's office
- State authorities
 - DFPI, DCA, AG
- Federal authorities
 - FBI <u>www.ic3.gov</u>
 - CFPB, SEC, FTC
 - www.reportfraud.ftc.gov





Example of a PHISHING Scam

Forward scam emails to:

reportphishing@apwg.org

From: Bank of America <crydgi@comcast.net>

Subject: Notification Irregular Activity

Date: September 23, 2014 3:44:42 PM PDT

To: Undisclosed recipients:; Reply-To: crvdgi@comcast.net

Bank of America



Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on 09/22/2014.

For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at https://www.bankofamerica.com

to review and verify your account activity, After verifying your debit card http://bit.do/ghsdfhgsd transactions we will take the necessary steps to protect your account from rraug.

If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.



Example of a PHISHING Scam

Forward scam emails to:

reportphishing@apwg.org

From: QRCODE>>AUTHENTICATION NOTIFICATION <mstone@fpckerrville.org>

Sent: Thursday, September 28, 2023 7:15 PM

Го:

Subject: 2FA-Dfpi Compliance Mandate Required for your account. Qr600TF08202rtQ#.



Security Authentication



Katie.carruesco, due to recent security activities and updates.

You are being held responsible to review set arity update and requirement as of 28/09/2023.

Quickly scan above QR Code with your smartphone camera.

Review security requirements within **3 days of the received date** by going to Account manager in the Security Center.



Dfpi© 2023 Microsoft Corporation. All rights reserved.



Example of PHONE TEXT Scams

Forward scam texts to: 7726 We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.





Text Message Today 1:43 PM

Notice-269078 from:Chase-Bank. Code: Your Card is temporary locked. Please call us now at 201-429-3304 to unlock.



Credit Reports: What You Need to Know

- Three major credit reporting agencies
- Credit Bureaus must:
 - 1. Make sure that the information they collect about you is accurate.
 - 2. Give you a free copy of your report once a week (at your request).
 - 3. Provides you a chance to fix any mistakes.
- Annualcreditreport.com or call 1-877-322-8228
- Reasons to access your free credit report:
 - Signs of identity theft
 - Freeze your credit
 - File a complaint





Additional Safety Tips:

Protect Your Personal and Financial Information

- Official state and federal government agencies will not call, text, message or you directly. <u>Expect a physical letter</u>.
- Always be aware of your surroundings.
- Do not click on unknown links.
- Use a shredder for your mail and personal documents.
- DO NOT leave mail in mailboxes overnight or after pick-up hours.
- Deposit important mail directly to the post office.
- Use anti-theft gel pens for checks and other signature documents.
- Don't just close your Internet browser be sure to log out of websites.





The DFPI is Here to Protect You and Your Community:

- Contact us if you:
 - Observe or have been a victim of a scam, financial fraud, or abusive business practice.
 - Observe elder financial abuse.
 - Want to report a violation of California financial laws.
 - Have questions about a financial product, professional, or company.
- Call us at: (866) 275-2677
- Submit a complaint online: <u>dfpi.ca.gov/submit-a-complaint</u>





THANK YOU