



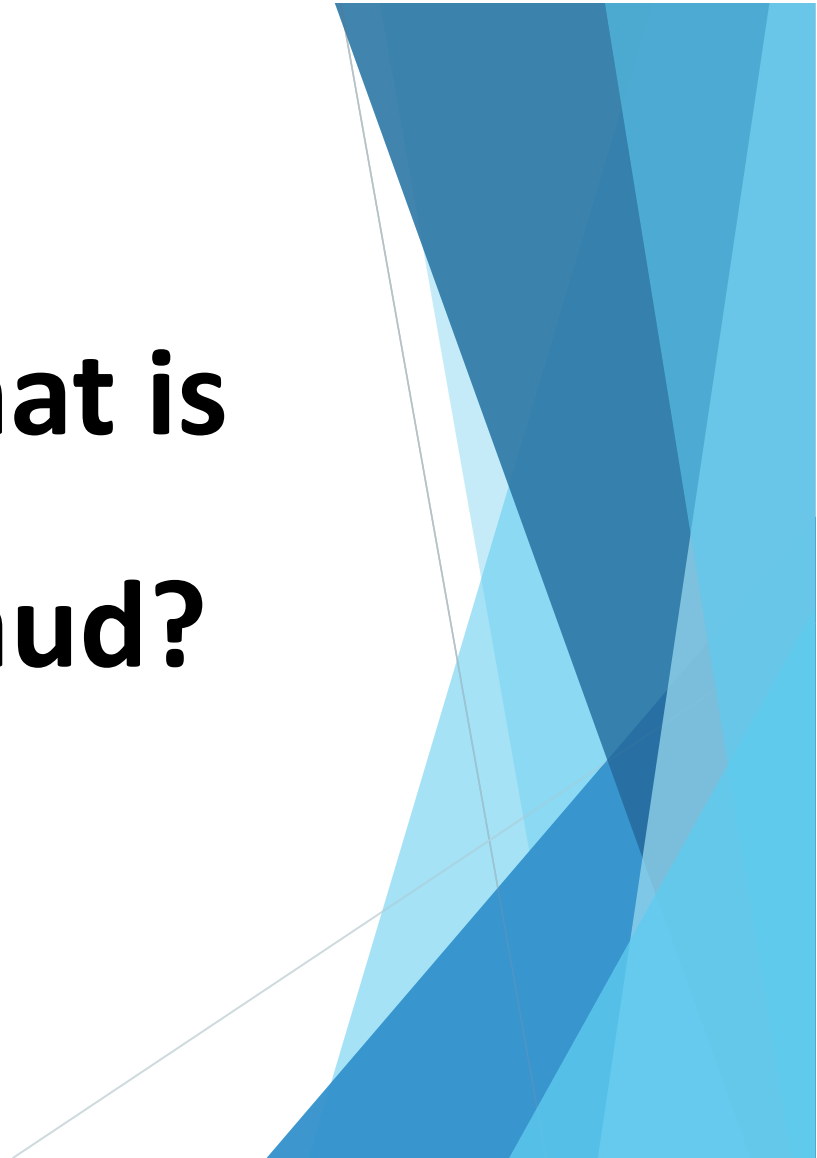
MALAGA
B A N K

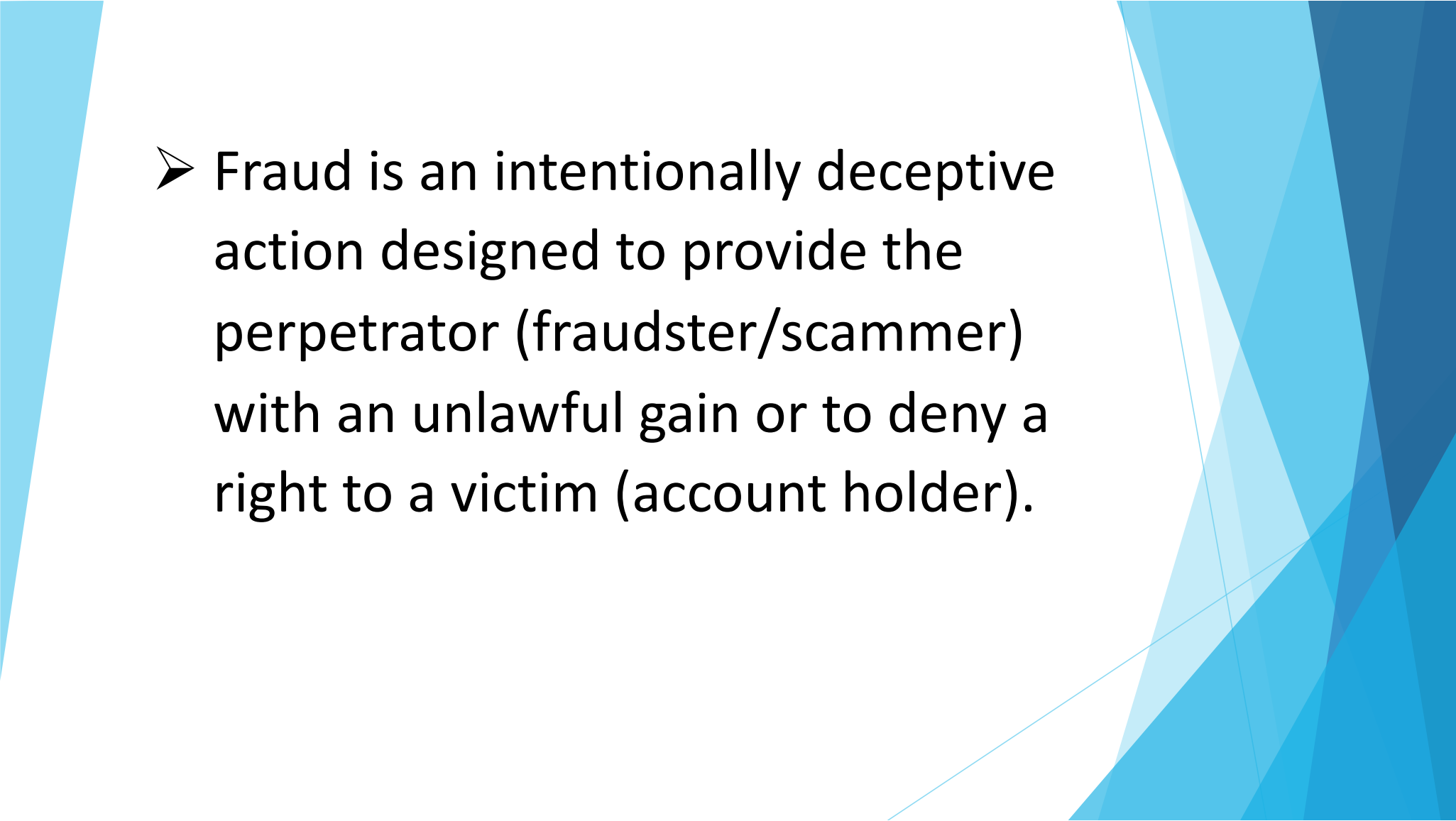
**Palos Verdes Estates
Annual Neighborhood Watch Meeting
November 5, 2023**



- Donald Lee, Senior Vice President/Risk Officer
- Rafael Vargas, Vice President/IT Manager
- Kryzla Serrano, Bank Security Officer/Special Projects



**What is
Fraud?**




- 
- Fraud is an intentionally deceptive action designed to provide the perpetrator (fraudster/scammer) with an unlawful gain or to deny a right to a victim (account holder).

- 
- 
- Criminals employ various tactics to deceive and manipulate their victims, often causing significant financial and emotional harm.



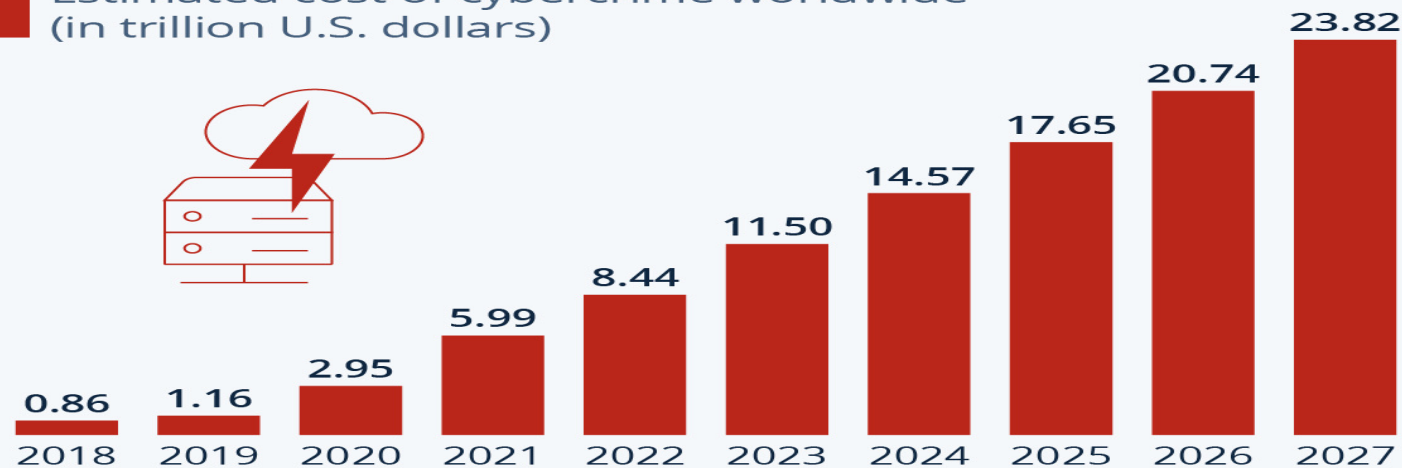
➤ Some common types of fraud include

- Cyber Fraud
 - Elder Fraud
 - Check Fraud
- 

Cybercrime vs Physical Crime

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF



statista

- Phishing attacks are the most common type of cybercrime, accounting for 300,497 complaints in 2022.
- Source: FBI

Number of reported robbery cases in the United States from 1990 to 2022



Sources

FBI; US Bureau of Justice Statistics
© Statista 2023

Additional Information:

United States; 1990 to 2022

Cyber Fraud (Cybercrime)

- **Phishing:** Scammers send fraudulent emails or text messages designed to trick victims into revealing personal information or clicking on malicious links.

- **Tech Support**: Scammers pose as tech support representatives to gain remote access to victims' computers, steal personal information, or install malware.



- **Malware/Virus**: Scammers trick victims into downloading malware/virus (or do it unknowingly), allowing them to access sensitive information or take control of devices.



➤ **Point of Sale (POS) Skimmers:**

Scammers will add a card reader device to the POS device, allowing them to intercept your card/account information.



Fraud Directed Toward Older People

- **Grandparent Scams**: Scammers impersonate grandchildren or other relatives in distress, requesting urgent financial assistance.
 - Artificial Intelligence (**AI**) – Don't Trust the Voice!
 - Hang up – Call loved ones directly

➤ **Investment Scams**: Scammers promise high returns on bogus investment opportunities, persuading victims to invest their money, which is then lost.



➤ **Other types of Fraud:**

- Romance Scams
- Lottery and Prize Scams
- Charity Scams
- IRS Scams



Check Fraud


- **Check Security Pens**
 - **Recommended – Gel pens**
 - **Avoid – Ball point pens**
- **Utilize Online Banking – Bill Pay**
- **Review Statements and Check Images frequently**

Check Fraud

- **Avoid Mail Drop Boxes – Hand mail to post office employee**
- **Report Mail Theft-Related Check Fraud to United States Postal Inspection Service at **(877) 876-2455** or <https://www.uspis.gov/report>**

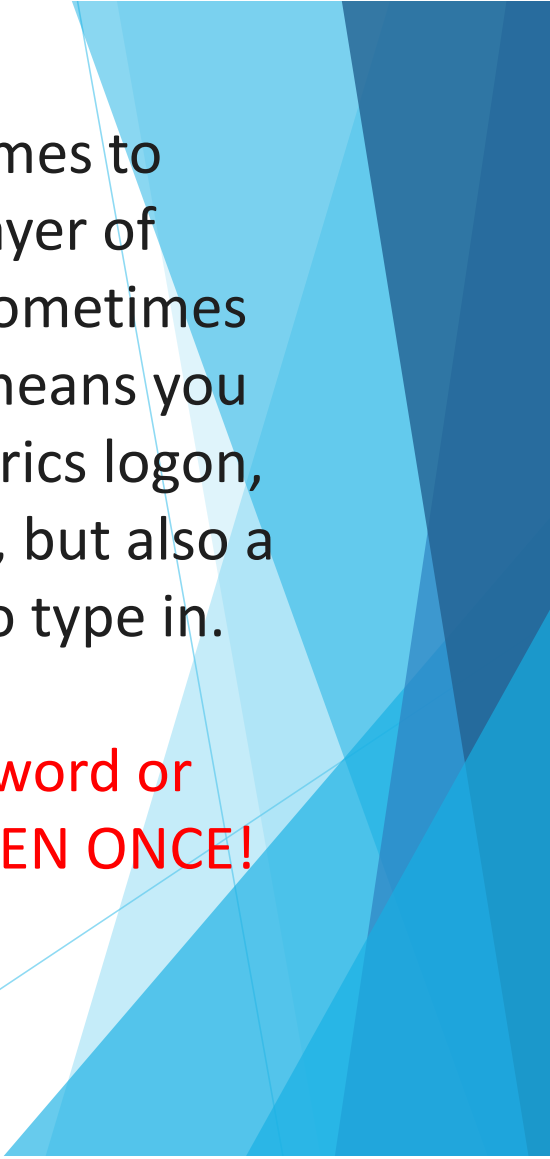
Fraud Protection

- **Education**: Stay informed about common scams and tactics used by criminals.
- **Software Updates**: Keep your devices and software up to date with the latest security patches.



➤ **Lock your Devices**: Use a passcode or fingerprint to lock your phone or tablet. If you have a computer, use a strong password that's at least 12 characters long.

➤ **Strong Passwords**: Create strong, unique passwords for all online accounts and enable **Multifactor Authentication** whenever possible.



➤ **Enable Multifactor Authentication:** When it comes to logging into your online accounts, add a second layer of defense by enabling multifactor authentication, sometimes referred to as “**two-factor authentication.**” This means you not only need a password or passcode (or biometrics logon, like a fingerprint or facial scan) to confirm it’s you, but also a one-time code you’ll receive on your cell phone to type in.

➤ **One-Time-Passcodes (OTP) – NEVER share password or One-Time Passcodes (OTP) with anyone – NOT EVEN ONCE!**

➤ **Reporting**: Report any suspicious activity or potential scams to the appropriate authorities. **Review Statements and Online Banking frequently!**



Fraud Protection Cont.

- **What do I do when Fraud occurs?**
 - 1. Contact your local branch immediately – Do not wait!**
 - 2. Freeze all accounts (temporary)**
 - 3. Complete applicable fraud/claim forms (e.g. Reg E Notification, Affidavit of Forgery)**

Fraud Protection Cont.

- **What do I do when Fraud occurs?**
 - 1. Scan computer/tablets/phones for virus and malware**
 - 2. Update email, username, and passwords on everything**
 - 3. Place a Credit Security Freeze and/or Credit Monitoring**

Real World Examples

- Online Banking (P2P & External Transfers) Fraud
 - Scammers are spoofing your banks phone number
 - Scammers will present themselves as your banks Fraud Department
 - Scammers use Phishing/Vishing technique to gain Account Holders credentials for Online Banking and initiate fraudulent transfers.
 - Personal information stolen/sold

➤ Check Mail-Theft Fraud

- Checks stolen from mail drop boxes
- Checks stolen in transit
- Checks altered/forged
- Account/Routing number sold in dark market
- Personal information stolen/sold



Resources

- **Malaga Bank's Identity Theft Booklet***
- **Malaga Bank website – Security Section***
- **www.annualcreditreport.com**
- **USPIS at (877) 876-2455 or
https://www.uspis.gov/report**

*Contains websites/links to various resources