50 YEARS OF TRUST

بنك برودا
Bank of Baroda
India's International Bank

FRAUD AWARENESS

KNOW IT. SEE IT. BE AWARE OF IT & REPORT IT

WHAT IS FRAUD?

"Wrongful or criminal dishonesty intended to result in personal or financial gain"

CAN FRAUD BE DONE BY MISTAKE?

YES

NO

WHO COMMITS FRAUD?…
WHY DO THEY COMMIT FRAUD?

Normal people do it!

- Greed
- Making bad decisions
- Presented with an opportunity
- Perception that they will not be detected
- For personal gain or to damage others

Psychology Behind Fraudulent Conduct

Pressure

Financial or emotional stress due to which the fraud is committed.

- Meet deadlines
- Addiction
- Family needs

FRAUD

Rationalization

Personal justification of dishonest actions.

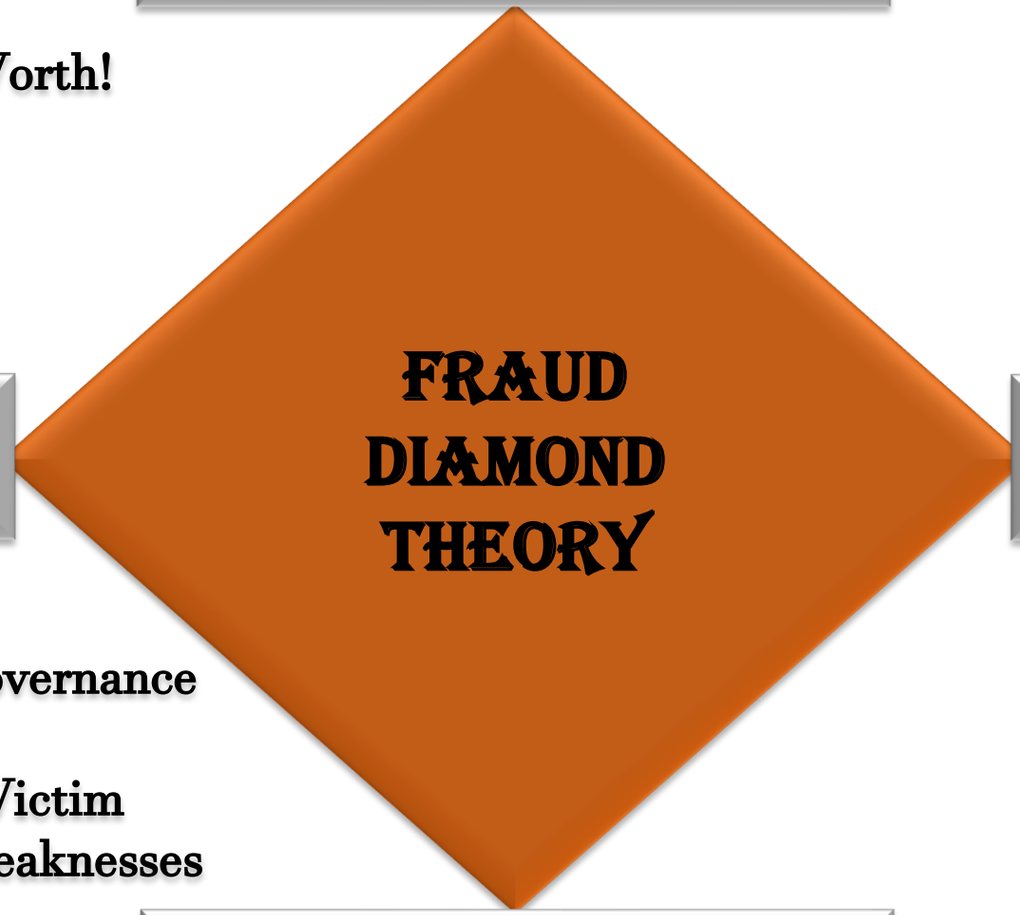
- I think it's okay
- Sounds reasonable
- I deserve

Opportunity

Ability to execute a plan due to weaknesses in an organization's internal controls or processes.

- Override
- Write-off
- Utilize funds from Dorman accounts

Fraud Diamond Theory



- Financial Pressure
- Monetary Gains
- Meet Deadlines
- Greed
- Pressure to perform
- Lifestyle Needs

- I Don't Get Paid What I Am Worth!
- Everyone Else is Doing It!
- I Intend to Pay it Back!
- Nobody Will Miss the Money!

- Internal Controls:
  - None in place
  - Not Enforced
  - Not Monitored
- No Segregation of Duties
- Too Much Trust
- Tone at the Top

- Knowledge about Corporate Governance
- Ability to Manipulate Others
- Technical Knowledge to Steal Victim Identities or Exploit Software Weaknesses

David T. Wolfe and Dana R. Hermanson, 2004

Types of Frauds

Internal Fraud:

Internal fraud, also known as employee fraud, occurs when employees or insiders of an organization engage in fraudulent activities to benefit themselves at the expense of the organization. This type of fraud is committed by people who have access to the company's assets and internal systems. Common forms of internal fraud include Embezzlement, Payroll Fraud, Expense Reimbursement Fraud etc..

External Fraud:

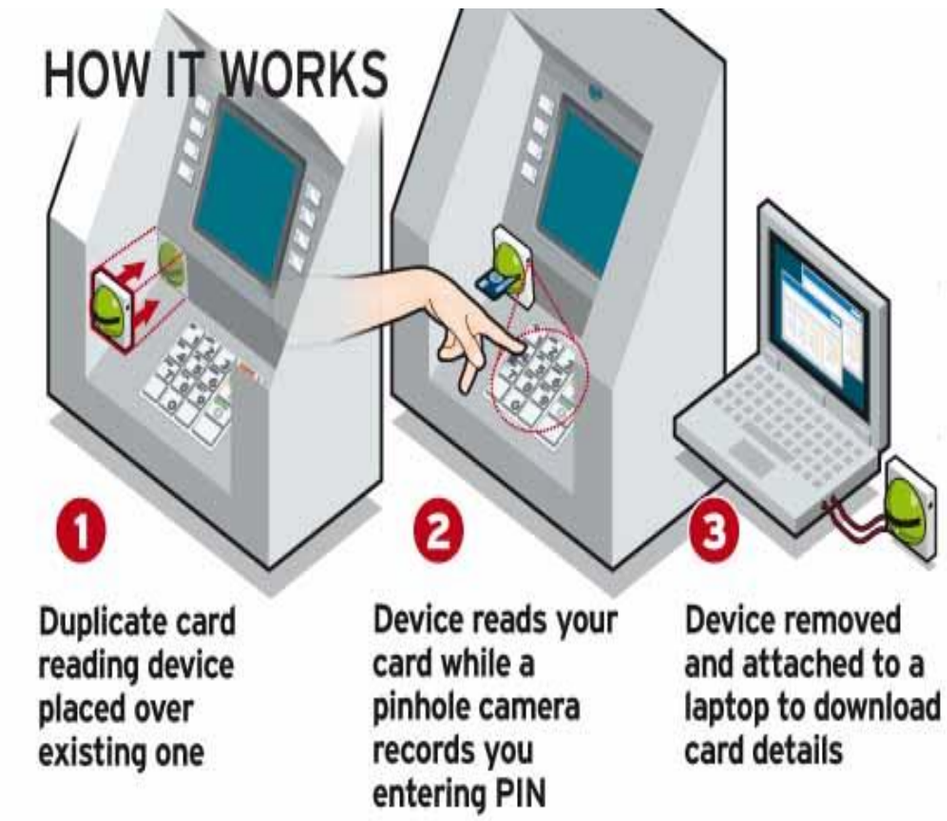
External fraud refers to fraudulent activities committed by individuals or entities outside an organization, aimed at deceiving or manipulating the organization for personal or financial gain. This type of fraud is carried out by outsiders who do not have authorized access to the company's internal systems or assets. Common forms of external fraud include Identity Theft, Phishing, Credit Card Fraud, Cyber Fraud etc..

ATM Frauds & Cyber Fraud

ATM Fraud

Skimming

Skimming is a method used by fraudsters to steal credit or debit card information during a legitimate transaction. It typically involves the use of a small electronic device, known as a skimmer, which is secretly installed on or near a legitimate card reader, such as those found on ATMs, gas pumps, or point-of-sale terminals.



Social Engineering Fraud

Phishing

Phishing is a type of cybercrime in which fraudsters attempt to deceive individuals into providing sensitive information, such as usernames, passwords, credit card numbers, or other personal or financial data, by impersonating a trustworthy entity or organization. This is typically done through deceptive emails, text messages, or websites that mimic legitimate sources.

Modus Operandi: Phishing attacks often involve sending out mass emails that appear to be from reputable companies, financial institutions, government agencies, or even friends or colleagues. These messages typically contain urgent or enticing requests tempting the recipient to click on a link, download an attachment, or provide sensitive information under false pretenses.

Clicking on the link takes the customer to a fake website that looks exactly like the official Bank website and the personal /banking information gets compromised once the victim fill and submits a web form with his/her information.

How to safeguard yourself from Phishing Fraud:

❑ Always check the web address carefully.

❑ Never click on any suspicious links received via email. Report the email to the organization & then delete the email.

❑ Do not divulge any sensitive or confidential information on email, even if the email seems to be from any government authorities or service providers

❑ Avoid opening unexpected email attachments or links.

❑ Using security software, such as antivirus programs and email filters, can provide an extra layer of defense against phishing attempts.

Social Engineering Fraud

Smishing

Smishing is a form of cyber attack that utilizes SMS (Short Message Service) or text messages to deceive individuals into providing sensitive information or taking specific actions. Similar to phishing, Smishing attempts often involve impersonating legitimate entities, such as banks, government agencies, or service providers, to trick recipients into divulging personal or financial information, clicking on malicious links, or downloading harmful attachments.

Modus Operandi: In a typical Smishing attack, recipients receive a text message containing a deceptive message, such as a fake alert about a compromised account, a prize or reward offer, or a request to verify account information. The message usually includes a phone number to call or a link to visit, which directs recipients to a fraudulent website or prompts them to provide sensitive information directly through the text message.

How to safeguard yourself from Smishing Fraud:

- One should be cautious when receiving unsolicited text messages, especially those that request sensitive information or prompt immediate action.
- Avoid clicking on links or downloading attachments from unknown or suspicious sources, and verify the legitimacy of any requests by contacting the organization or individual directly through official channels.
- Additionally, using security software on mobile devices can help detect and prevent Smishing attempts.

Alert On Smishing From Dubai Police & Smishing Attempt

Bank of Baroda
India's International Bank

Dubai Police شرطة دبي
@DubaiPoliceHQ

Never send money or share your bank details to online strangers. Protect yourself and data while using social networking sites.
#Protect yourself against social media scams.

#YourSecurityOurHappiness
#SmartSecureTogether #DPAwareness

WhatsApp

18:47

3 +971 50 211 8451

Today

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

1 UNREAD MESSAGE

عزيزالعميل.
، تم حظر بطاقة الصراف الآلي الخاصة بك. لأنك لم يكن لديك حتى الآن التحديث. إذا كنت تريد عمل بطاقة الصراف الآلي الخاصة بك بشكل صحيح ، فاتصل بهذا الرقم على الفور ٠
0543688390

Dear coustmor, your ATM card has been blocked. because you did not have an update yet.if you want your ATM card to work properly, then contact this number x to,
0525305112
https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.guide2dubai.com/directory/banks-344&ved=2ahUKEwjWi8Gu7_3dAhXmz4UKHblNBilQFjAXegQIBxAB&usg=AOvVaw2hUw0aODbSWE7aFDK_zm8y
17:57

Text Message

08:08 LTE

+92 330 2893578 >

Text Message
Thu, May 23, 13:06

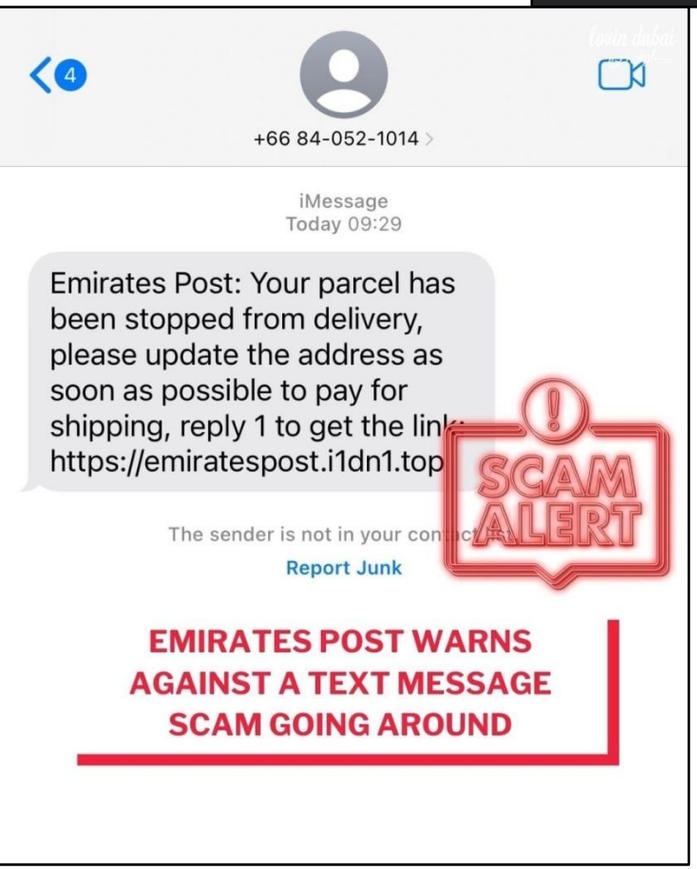
Dearcustomer your ATM card has been blocked because you do not have the updates after you cal ,,this number"0525018130,, - Sent via Lantech Soft

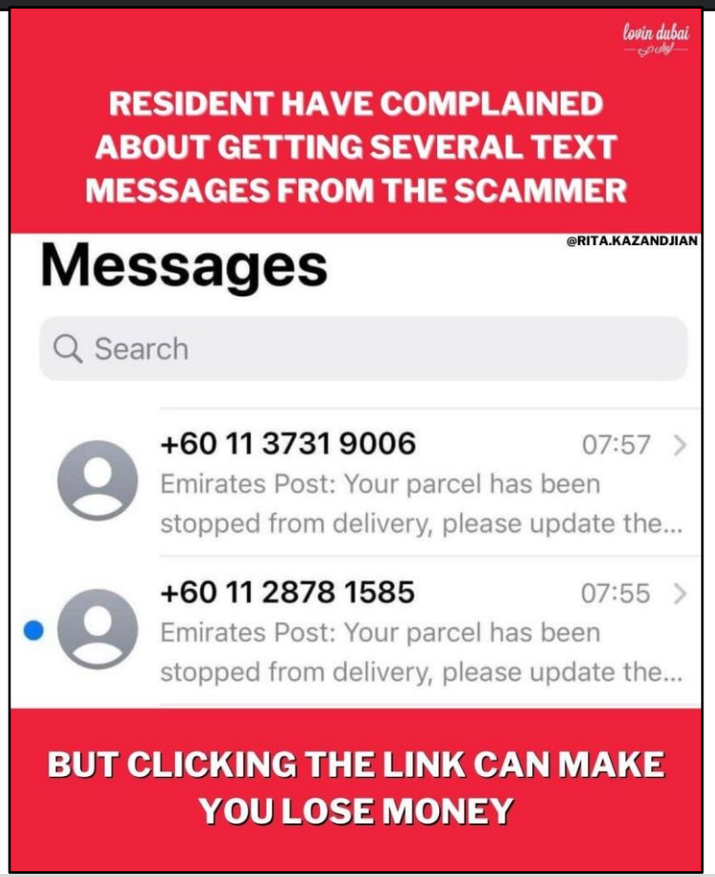
Text Message

Smishing Alert- Emirates Post (2023)

Lovin Dubai
1 h ·

Several residents have been receiving a suspicious text messages from a scammer pretending to be Emirates Post. Beware of this message as interacting with the link may cause you to lose huge sums of money. #lovindubai





Social Engineering Fraud

Vishing

Vishing, also known as voice phishing, is a type of cyber attack that involves using phone calls or voice messages to deceive individuals into providing sensitive information or taking certain actions.

Modus Operandi: In a Vishing attack, the attacker typically impersonates a legitimate entity, such as a bank, government agency, and uses social engineering techniques to manipulate the victim into divulging personal or financial information. The attacker may claim there is an urgent issue with the victim's account, offer a fake prize or reward, or request verification of account details under false pretenses.

How to safeguard yourself from Vishing Fraud:

- ❑ It's important to be cautious when receiving unsolicited phone calls or voice messages, especially those that request sensitive information or demand immediate action.
- ❑ Never provide personal or financial information over the phone unless you have verified the legitimacy of the caller through official channels.
- ❑ Additionally, be wary of caller ID spoofing, where attackers manipulate the caller ID to appear as if the call is coming from a trusted source
- ❑If you suspect a Vishing attempt, hang up and contact the organization or individual directly using contact information from their official website or documentation.

Telecom Fraud

SIM Swap

SIM swapping, also known as SIM hijacking or SIM card swapping, is a type of cyber attack in which an attacker fraudulently obtains control of a victim's mobile phone number by convincing the victim's mobile carrier to transfer it to a replaced SIM card controlled by the attacker.

Modus Operandi: The process typically involves the attacker gathering personal information about the victim, such as their name, address, date of birth, and social security number, through various means such as phishing, social engineering, or data breaches. Once the attacker has enough information, they contact the victim's mobile carrier posing as the legitimate account holder and request that the phone number be transferred to a new SIM card, usually claiming that the original SIM card was lost or damaged.

If successful, the mobile carrier deactivates the victim's original SIM card and activates the new SIM card provided by the attacker, effectively transferring control of the victim's phone number to the attacker's device. With control of the victim's phone number, the attacker can intercept incoming calls and text messages, bypassing two-factor authentication (2FA) codes sent via SMS and gain unauthorized access to the victim's online accounts, including email.

How to safeguard yourself from SIM Swap fraud:

- ❑ If your mobile number is not working for longer than the usual period, then immediately inquire with your mobile operator to make sure you haven't fallen victim to some evil fraud.
- ❑ Always Register for SMS and Email Alerts to get regular update about the activities in your bank account, even if it is chargeable.
- ❑ Check your bank statements and transaction history for any irregularities on a regular basis.

Cyber Fraud

Identity Theft

Identity theft is a type of crime in which an individual's personal or financial information is stolen and used by someone else without their permission, typically for fraudulent purposes. This stolen information can include identification documents, credit card numbers, bank account details, passwords.

Modus Operandi: The personal information of an individual is gathered through various other means such as Phishing, Vishing, Smishing or any other means.

Once they have access to the victim's personal information, they can use it to apply for new credit cards, accounts, make unauthorized purchases, apply for loans or even commit crimes under the victim's identity.

How to safeguard yourself from Identity Theft Fraud:

- ❑ Always shred or destroy any paper or envelope containing personal identifiable information.
- ❑ Never share your personal information with a stranger or any third party, posing as a bank representative. Cross check the identity of a person posing as bank staff directly with bank branch or head office, not on numbers they provide for verification.
- ❑ Always update your mobile/contact number, email ID and identification documents with your bank in case they have change.
- ❑ **"Verification"** and **"Due Diligence"** are the key factors to mitigate the risk derived from Identity Theft fraud.

Social Engineering Fraud

Business Email Compromise (BEC)

Business Email Compromise (BEC) is a type of cybercrime where an attacker targets businesses to fraudulently gain access to sensitive business information or funds.

1. **Email Account Compromise**: The attacker may hack into a legitimate business email account or create an email account that looks similar to a legitimate one.

2. **Phishing and Social Engineering**: They use phishing emails or other social engineering techniques to deceive employees or business partners. These emails often appear to be from a trusted source, such as a CEO, CFO, or a business partner.

3. **Fraudulent Requests**: The attacker then sends emails from the compromised or spoofed account to employees within the company, requesting actions like transferring funds, providing sensitive information, or changing payment details.

4. **Exploitation**: If the employees follows through with the request, the attacker gains access to the requested funds or information.

Business Email Compromise (BEC), Case Study- CEO Fraud

Company: XYZ Corporation
Target: Jane Scott, CFO of XYZ Corporation
Attacker: A cybercriminal impersonating the CEO of XYZ Corporation, John Smith

Stage 1: Research and Target Identification:

The attacker spends several weeks gathering information about XYZ Corporation and its key employees through public sources like LinkedIn, the company's website, and social media. They identify Jane Scott, the CFO, as a key target who has the authority to authorize large financial transactions.

Stage 2: Email Compromise or Spoofing:

The attacker creates an email address that looks very similar to the CEO's actual email address. The legitimate email address is **john.smith@xyzcorp.com**, and the attacker's spoofed email address is **john.smi1th@xyzcorp.com**.

Stage 3: Social Engineering:

The attacker crafts an email to Jane Scott that appears to come from John Smith. The email is marked "**Urgent**" and is written in a style similar to the real CEO's typical communication.

Email Subject: Urgent: Immediate Wire Transfer Required

Business Email Compromise (BEC), Case Study- CEO Fraud

Email Body:

Hi Jane,

We are in the final stages of a confidential and time-sensitive acquisition, and I need you to process an urgent wire transfer of $250,000 to our new business partner. This is extremely important and must be done today without delay.

Please transfer the funds to the following account:

Bank: ABC Bank
Account Name: XYZ Holdings
Account Number: 123456789
SWIFT Code: ABCDUS33

Once the transfer is complete, send me the confirmation receipt. Do not discuss this with anyone else in the office as it is highly confidential.

Thank you,
John Smith
CEO, XYZ Corporation

Business Email Compromise (BEC), Case Study- CEO Fraud

Stage 4: Convincing the Victim:

Jane Scott receives the email and, recognizing it as coming from the CEO (or so she believes), feels the urgency and importance of the request. The email's language and format match the CEO's usual style, and the stress on confidentiality adds to the pressure.

Stage 5: Monetary Transfer Request:

Believing the request to be legitimate, Jane proceeds with the wire transfer to the specified account.

Stage 6: Follow-Up and Persistence:

After the transfer, the attacker may send a follow-up email thanking Jane and reminding the confidentiality of the matter, further reducing the likelihood of her mentioning it to others.

Stage 7: Money Laundering:

Once the funds are transferred, the attacker quickly moves the money through various accounts to vague the trail and makes it difficult to recover the funds.

Business Email Compromise (BEC), Case Study- CEO Fraud

Stage 8: Covering Tracks:

If the attacker had access to the CEO's actual email account, they might delete the sent email and any related correspondence to minimize the chance of detection.

Outcome and Response:

A few days later, John Smith (the real CEO) might casually mention the acquisition during a meeting, leading Jane to realize something is wrong. She checks her emails and finds no mention of the wire transfer from the CEO's legitimate email account. Realizing she has been duped, Jane immediately contacts the bank to attempt to recall the funds, but it might be too late.

XYZ Corporation would then report the incident to law enforcement and possibly engage a cyber security firm to investigate the breach and strengthen their defenses.

Business Email Compromise (BEC), Case Study- CEO Fraud

How to safeguard from Business Email Compromise Fraud:

Verification Procedures: Implementing strict verification processes for financial transactions, such as multi-factor authentication and confirmation via multiple communication channels, such as a phone call or an in-person confirmation.

Employee Training: Regularly train employees to recognize phishing and social engineering tactics.

Email Security: Using advanced email security solutions to detect and block phishing and spoofing attempts.

Incident Response Plans: Having a clear plan for responding to BEC incidents, including immediate action to halt transactions and reporting to authorities.

Money Laundering Conspiracy

Money Mule

A money mule is a person who is recruited, often unknowingly, by criminals to transfer illegally obtained money between different accounts or jurisdictions. Money mules are typically used as intermediaries to launder money obtained through various illicit activities, such as online scams, identity theft, phishing, or cybercrime.

Modus Operandi: Scammers contact victims via emails, chat rooms, job websites, or blogs, persuading them to accept money into their bank accounts in exchange for promised commissions. Afterwards, the scammers transfer the illicit funds into the mule's account..

The subsequent action involves directing the victim to transfer the funds into another mule's account, ultimately leading to the transfer of the money to the fraudster's account. When such fraudulent activities are reported to the police, the money mule becomes the focus of police investigations

How to safeguard yourself from Money Mule Fraud:

- ❑ Never respond to emails asking for your bank account details.
- ❑ For an overseas job offer, first confirm the authenticity and contact details of the company offering the job.
- ❑ Do not get greedy on getting attractive offers/commissions or do not agree to receive unauthorized money.

Magic Ink Fraud

The writing from these "magic ink" pens vanishes once the cheque is subjected to heat or can be effortlessly erased using a special eraser provided with the pen. After erasing the original amount and beneficiary name, the fraudster alters both, allowing them to cash the cheque.

Forgery & Counterfeiting

Forgery

Forgery is the act of falsely making, altering, or imitating documents, signatures, works of art, or other items with the intent to deceive or defraud. Common examples include forging a signature on a cheque or creating a fake account statement.

Counterfeiting

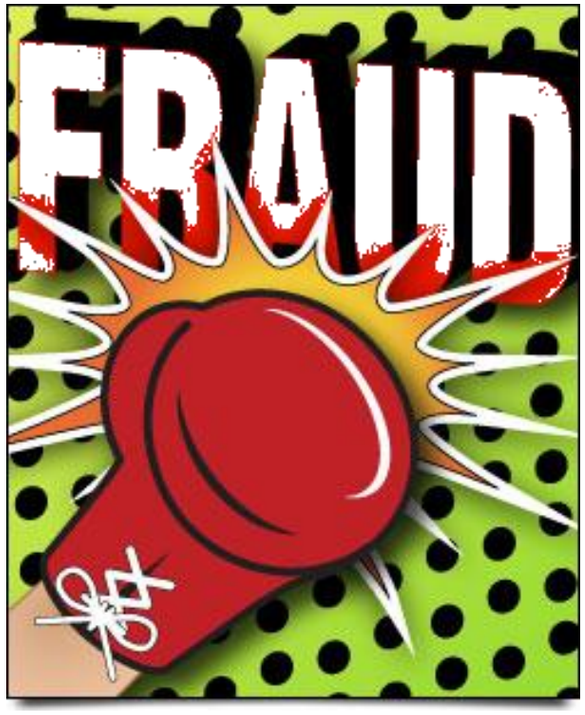
Counterfeiting is the act of creating imitation goods, currency, documents, or other items with the intent to deceive others into believing they are genuine. Common examples include producing fake money, creating knock-off designer products.

- ✓ Security features helps to identify forgery.
- ✓ Different security features for different documents.
- ✓ The more critical the document, the more security features are invested, to reduce the fraud likelihood.

Contact us !

Any inquiry please contact us on

Email: aldrin.earl@bankofbaroda.com
Name: Aldrin Gerard Earl
Mobile: +971554030829



Together Let's Fight Fraud!

50 YEARS OF TRUST

بنك برودا
Bank of Baroda
India's International Bank

Thank You