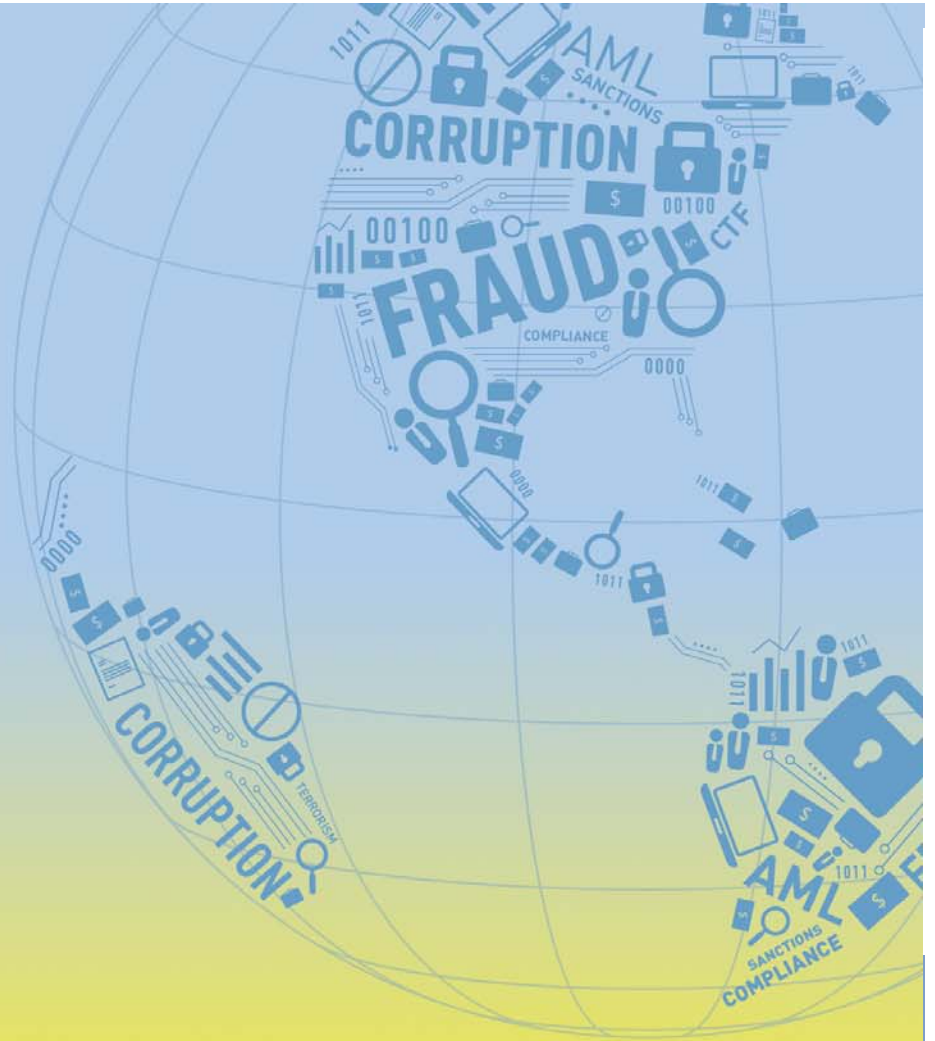




ASSOCIATION OF
CERTIFIED FINANCIAL
CRIME SPECIALISTS

A BARBRI Professional Association



Recognising Financial Frauds

- You are looking at investing your funds in high return, aggressive and high-risk investment scheme. Which scheme would you opt for -
 - Option A –Equity scheme assures high returns consistently in future. Past Investment statements show persistent performance contrary to market trends. No fees structure.
 - Option B –Equity scheme offers decently good returns outperforming most other equity funds in the market. However, the past performance shows that returns have been volatile and vulnerable to stock markets performance. Fee structure is 2% to 3%, similar to that of other schemes in the market.
 - Option C- Scheme is balanced fund – Allocation to equity and debt is done depending on the call of the fund manager anticipating the trend in the equity markets. When markets are plummeting, he switches to debt and vice-versa.

Fraudulent Investment Schemes

- **Ponzi-schemes** – Investment schemes that promise to pay relatively high rates of returns consistently. Fraudulent investment plans wherein new investments are used to pay off earlier investors.
- **Pyramid Schemes** - Schemes which promise consumers or investors large profits based primarily on recruiting others to join their program, not based on profits from any real investment or real sale of goods to the public.



Review this -

The CFO of a large public corporation sees that the Company's quarterly numbers are going to exceed analyst's expectations and it is very likely that the stock price will make a big jump. He mentions the earning reports to his wife, and she buys 1000 shares of the Company through her broker without any mention of what her husband told her.

Her broker, knowing that she is the wife of CFO, recommends to all his customers to buy the shares of the Company.

Is insider trading committed?

If yes, who would be held responsible?

- The CFO
- The CFO's wife
- The stock broker
- The stock brokers customers who bought shares

Securities Fraud

- Market manipulation scheme
 - Pump-and-dump schemes
 - Short-selling or Scalping schemes
- Insider Trading
- Stock options fraud
- Equity Crowd funding via Internet
- Fake deposit certificates

Real Estate

A buyer is attempting to obtain a large mortgage on a home from your institution. He is seeking to purchase the home as an investment property. The buyer has been behaving erratically and has been difficult to contact at times.

Below are facts of the case –

- A. A real estate agent from a nearby city is helping to broker the sale
- B. The seller is not currently listed as the occupant of the property
- C. The buyer currently has a large mortgage outstanding on his own property
- D. The buyer has no previous history of obtaining mortgages from your institution

Is any fact indicating that the buyer may be committing mortgage fraud?

Mortgage & Loan Fraud

- Collaboration with property appraisers or others
- Inflation of property
- Intentional material misrepresentation or non-disclosure of facts
 - Income Fraud
 - Employment Fraud
 - Occupancy Fraud
 - Appraisal Fraud
 - Shot-gunning Fraud
 - Cash back Fraud
 - Buy and bail Fraud

Insurance Fraud

A major insurance company has recently noticed a pattern of potentially suspicious transactions. Their long-time customer is employed in a consulting position that requires her to travel internationally on an unpredictable schedule and she often resides overseas. The customer has several properties insured with the company for large amounts. In the past three years, she has overpaid her premiums numerous times and then requested a refund be issued. The following are facts about the customer -

- A. The customer often requests that refunds be made by wire transfer to banks outside of the country.
- B. The customer makes the overpayments at different times of the year and in varying amounts.
- C. The customer has recently taken out a sizeable new insurance policy on a commercial property with your company.
- D. The customer has requested that refunds on excess premiums be made to an offshore corporation.

Given the above facts, should one investigate or not? If yes, why?

Other Common Frauds

- **Credit & debit card frauds**

- **Skimming** - This involves stealing information off a credit card during a legitimate transaction.
- Stolen cards or credit card details

- **Advance fee scams** –A letter, email or phone call offering you a large sum of money if you can help someone transfer millions of rupees or other currency out of his country.

- **Fake prizes / International lottery fraud** - A perpetrator claims that you have won a non-existent prize. You are asked to send a cheque/give credit or debit card details to pay the taxes shipping and handling charges.

- **Fund Transfer scams** -You are asked through an advert or email to receive a payment into your bank account, and to send it abroad in return for receiving a commission

- **Inheritance scams / Wills and legacies scam**- Receive a mail from an '*estate locator*', *advocate*, '*research specialist*' purporting an unclaimed inheritance / refund / advisory fees to obtain claim.

Recent Case Studies

Recent Fraud -

1MDB (Malaysian Development Bernard) – One of the world’s largest Fraud

- Money stolen from a Malaysian sovereign wealth fund . Funds stolen from 1MDB helped finance several major motion pictures, including Hollywood A-lister Leonardo DiCaprio’s “The Wolf of Wall Street”.
- Misappropriation of 1MDB funds was accomplished with an extravagant web of lies and bogus transactions.
- Billions of dollars that should have been used to help the people of Malaysia.
- While the tactics were sophisticated, the goal of the scheme was simple: get funds from the bank and governments in the form of bonds, loans and other structures, and instead of using the money to help Malaysians, misappropriated them.
- Then, made it look like the money is going to big companies that are doing the right thing with funds, or at least growing them .
- **Creating shell companies, the name is the game**
 - “Aabar-BVI” was created and named to give the impression that it was associated with Aabar Investments PJS,” a subsidiary of the Abu Dhabi investment fund IPIC.
 - Created a company called Blackstone, to make it appear linked to billion-dollar real estate giant Blackstone.

Recent Lottery Fraud

- Eddie Tipton, the mastermind of a scheme rocked the lottery industry.
- Tipton's brother wrote and installed code for software that picked random numbers for games sold by its member lotteries.
- Investigators say Tipton designed his code so that on three days of the year, he could predict winning numbers in some games.
- The Tiptons and friend Robert Rhodes bought winning numbers for drawings in Colorado, Wisconsin, Iowa, Kansas and Oklahoma between 2005 and 2011.
- The conspiracy unravelled after Tipton was caught on surveillance video buying a winning \$16.5 million ticket in December 2010 in Iowa that he, Rhodes and others unsuccessfully tried to claim.

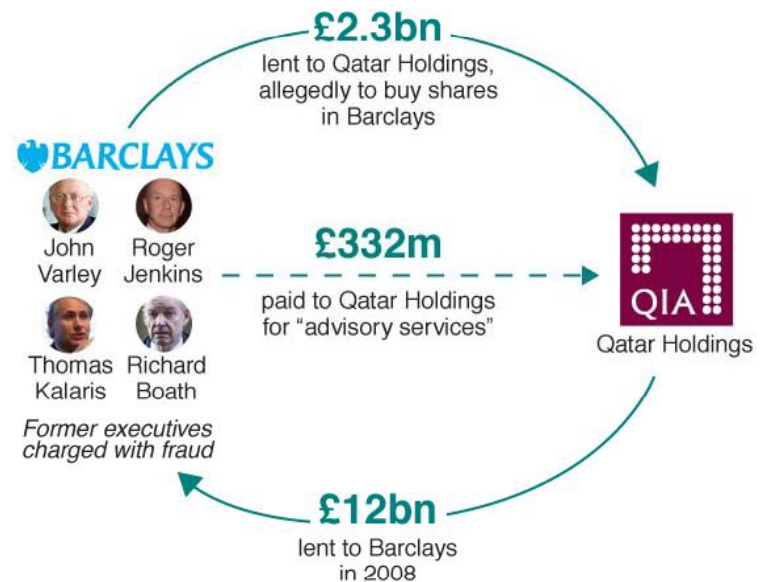
Barclays Fraud

Barclays gets sued in Qatar

Barclays and four former executives have been charged with fraud over their actions in the 2008 financial crisis.

The Fraud involved the way the bank self-raised billions of pounds from Qatari investors enabling it to avoid a government bailout.

Barclays: The Qatari connection



BBC

Cyber Fraud

Characteristics of Phony Mails & Calls

- Attempts to obtain valuable information through various means is called “phishing”. Means could be emails, websites, phone etc.
- Request for revealing personal information such as credit card number, date of birth, ATM pin etc. Most genuine companies/banks never ask their customers to submit confidential data via any means.
- Create a sense of urgency – most phony emails/calls demand immediate action. Emails saying your account will be deactivated in a day if you don’t enter your credit card number is an example.
- Generic salutation – Phishing emails generally start with a *Dear customer* instead of the user’s name.
- Attachments – Phishing emails might have attachments which will mostly contain malware.
- There’s a good chance that phishing emails might contain bad grammar and spelling mistakes.

Characteristics of Phony Links & Websites

Most of us click links without a second thought. However, some links are Phony and might show something else but will actually direct to a different location.

- [Phishing emails](#) use various methods to hide the actual URLs.
- The link that is displayed will be an image while the actual link could be different.
- Actual links can be masked using HTML. Thus, the text displayed will be *http://websitename.com/* while the hyperlink set will be *http://www.thersite.com*.
- Links using @ in the link are sometimes phony. If a link contains the '@' sign, the URL you're taken to will be the one after the '@' sign. Eg. If the link is *www.microsoft.com/windows@web.com/?=true*, the actual URL you will be taken to is *web.com?=true*.
- Links with numbers instead of the website name. Example: *www.182.11.22.2.com*.
- Shortened URLs which appear as *http://bit.ly/1UTZzTI*. These are usually long and may hide suspicious elements like malware.

Stay safe & protected

- Legitimate websites use SSL for protecting your information when entering your data. Make sure that the URL starts with *https://* instead of *HTTP://* for pages where you have to submit username/password or other private information.
- Use a browser that comes with phishing protection such as the latest versions of IE, Firefox, Opera, Chrome etc. They come with blacklists of known phishing sites that are updated regularly and if you happen to visit any of these sites, they will alert you.
- Use a good upto date anti-virus and update the version from time to time.
- Take use of your Email provider's spam filters

Spot Fake News

Ask basic questions -Who made this? Who is the target audience?

- Who paid for this? Or, who gets paid if you click on this?

- Who might benefit or be harmed by this message?

-What is left out of this message that might be important? Is this credible ? Why ?

Few technical things to watch for:

- Look for unusual URLs or site names, including those that end with “.co”
- Look for signs of low quality - words in all caps, headlines with glaring grammatical errors, bold claims with no sources, sensationalist images etc.
- Check a site’s “About Us” section. If this information doesn’t exist — and if the site requires that you register before you can learn anything about its backers — you have to wonder why they aren’t being transparent.
- Check Wikipedia, and Google before trusting or sharing news that seems too good (or bad) to be true. Consider whether other credible, mainstream news outlets are reporting the same news.
- Check your emotions- Anger /excitement. Clickbait and fake news strive for extreme reactions

Combating Financial Frauds

Evolution of Financial Frauds

1990-1999

- Hawala Transactions
- Ponzi schemes
- Fake currency
- Cheque forgery
- Dealing /advancing loans without adequate due diligence
- Siphoning of investors' money through fictitious companies
- Use of fictitious government securities

2000-2016

- Cybercrime
- Debit & credit card fraud
- Tax evasion and money laundering
- Hacking & Identity theft
- Terrorist financing
- Data security
- Bribery & corruption
- Tax shelters & vehicles
- Collusive frauds
- Benami & fake demat accounts etc...

Advance of technology has spurred growth and made it a global menace

Common element of most financial frauds

Four phases of financial fraud :

1. Crime is planned for some economic advantage
2. Crime is committed
3. Proceeds from crime are laundered
4. Victims are identified and recovery efforts are made

Money laundering is the common element of most frauds.

Stages of Money Laundering

The three stages of money laundering are :

1. Placement
2. Layering
3. Integration

Placement stage is most vulnerable to detection.

Common Means

- Account takeover or account hacking
- Identification Fraud
- Misrepresentation or non-disclosure of facts
- Collusion between customer and fraudster
- Creating fake online identities
- Social engineering
- Leveraging technology (malware, phishing, vishing, smishing etc.)

Common Vehicles

- Special Purpose Vehicles/ Entities
- Shell companies
- Shelf companies
- Offshore Trusts / Entities – International Business Companies
- NGOs , Charitable organisations
- Real estate, expensive vehicles etc.
- Financial Institutions- Correspondent banks, Money transmitters, Private Banking, security brokers/dealers, financial instruments like bearer bonds.
- Non-Financial Institutions – Insurance, casinos, dealers in precious metals, art, hawala and other informal transfer system.

Indian Regulations

- Growing financial fraud cases, recent stock market scams, failure of non financial banking companies, phenomena of vanishing companies and plantation companies and failure of the regulatory mechanism to curb it has forced the Government of India to form Serious Fraud Investigation Officer (SFIO) under the Ministry of Corporate Affairs.
- The SFIO is a multidisciplinary organization having experts from financial sector, capital market, accountancy, forensic audit, taxation, law, information technology, company law, customs and investigation.

The Indian Laws & Regulations which refers to Forensic Accounting:

- **The Companies Act, 2013: Section 7(5), 36, 75(1), 206 (4), 213, 229, 251(1), 339 (3), 448 will attract liability under Sec 448 etc.**
- **SEBI Act :** Regulation 11 C of the SEBI Act, 1992 empowers the SEBI to direct any person to investigate the affairs of intermediaries or brokers
- **The Prevention of Money-Laundering Act**

About ACFCS & Cybint – Certification & Training

A Step Ahead with ACFCS

Association of Financial Crime Specialists (ACFCS), USA, is a leading provider of practical tools and knowledge to help professionals improve results in financial crime detection and prevention.

Financial crime comes in many different forms — a corrupt public official accepting bribes, a narcotics cartel laundering illicit proceeds, a fraudster running Ponzi schemes or a terrorist financier. ACFCS recognizes that these seemingly diverse types of financial crime are more alike than different, and strives to help you stay a step ahead of these intersections.

Why ACFCFS?



Highlights

- Better performance in financial crime
 - Compliance
 - Investigations
 - Regulation and
 - Enforcement.
- Strong advisory board and financial crime experts
- Financial Crime 360 e-zine, webinars & forums keep you posted on current news & trends
- updated content,
- World wide recognition. CFCS professionals in over 83 nations.
- Other international and domestic certifications not as comprehensive and integrated

Cybint

- ACFCS has also introduced Cybint under their umbrella, which provides niche training programs in “Cyber discovery” and “Cyber protection”.
- More than 75 training programs on how to reduce cyber threats, how to get access to critical data and information for their business.
- Has a smart tool-kit integrated in it, so you get access to relevant tools to implement what you studied in the program.

Cybint Protection

- Hardware exploits
- Wifi security
- Identity threats
- Cyber attacks- wares and viruses
- Privacy essentials, Social engineering, phishing etc.

Cybint Discovery

- Online research and investigations
- The finder- advanced search, hidden data
- Profiling and due diligence
- Meta data & digital forensics
- Geo location tracking. Darknet. Criminal trade etc.

Professions to which it adds Value

- Compliance officers – AML/BSA, fraud, anti-corruption, etc.
- Company secretaries- Ensuring compliance measure taken and incorporated
- Law enforcement – investigators, analysts, agents
- Regulatory agencies
- Forensic accountants
- Asset recovery specialists
- CAs, Auditors
- Private investigative professionals
- Financial Consultants
- Attorneys, legal professionals
- Bankers, Tax and other financial advisors
- Venture Capital Funds, PE's, Portfolio managers and other managing overseas funds
- Insurance Companies

Benefits to Individuals & Organisations

For Organisations

- Meaningful credit if violation occurs
- Exposure to International laws- FCPA, FATCA, UK bribery Act
- Knowledge about international organisations, associations, conventions, high risk jurisdictions, PEPs, Know your Employee program, International Agreements and Standards, Compliance programs, Interpretation financial documents, risk management, fraud detection and prevention.

For individuals

- Apart from knowledge enhancement, adds CFCS credential to your name
- Global certification recognised world over
- Very good career opportunities, opening up several avenue
- It will give an edge for jobs

Ajcon Global Services Ltd. & ACFCS

- Ajcon Consultants, a group Company, is the sole representative of ACFCS in India.
- The Company is listed on the BSE and provides a whole gamut of financial services including stock broking, loan syndication, insurance, Mutual funds, corporate advisory and merchant banking services.
- The Company is headed by Dr. Ashok Ajmera, a well known Chartered Accountant and market expert with 40 years of experience, and has established his footprints in the industry through his articles, TV interviews, prestigious posts and networking.
- Ajcon is looking at establishing a strong network of financial crime specialists in India by promoting education and training of ACFCS & Cybint programs.
- Being the sole representative, we are authorised to offer huge discounts, form chapters, hold discussions forum and organise speaker meetings.

THANK YOU