1. WHAT IS FRAUD?

Fraud is a crime of persuasion where the victim willingly participates with the criminal. It has been called “a theatrical mugging” and involves a wide range of psychological, societal, and economic principles along with human nature, creativity, and a unique set of skills and practices. There are no weapons, no criminals with masks, no physical intimidation, no dark alleys. In Perrow’s accident schema, fraud is tightly coupled and complex, making it hard to predict and sometimes detect; “Complexity and coupling only made deception easier and the consequences more extensive” (Perrow, 2010: 309). Fraud is wrongful or criminal deception for financial or personal gain. Fraud is described by a number of related terms. One is con (short for confidence game), an instance of deceiving or tricking someone or persuading someone to do or believe something, typically by use of deception. Another word used as a cognate of fraud is scam, a dishonest scheme where someone is deprived of valuables or possessions through deception (also thought of as a swindle). And even the simplest fraud requires strategy, operations, and tactics, typically called a scheme, a large-scale systematic plan or arrangement for attaining some particular object or putting a particular idea into effect, especially in a devious way or with intent to do something illegal or wrong. Thus, fraud is the wrongful or criminal deception for financial or personal gain. One who perpetrates a fraud is called a fraudster. Fraud can occur as a byproduct of the fraudster’s job and their access to work resources (crime at work), as a primary means of making money (crime as work), or a combination of both (crime after work). Like most other activities, the digital life and the internet make fraud easier (Byrne and Kimball, 2017). As noted former fraudster Frank Abignale explains:¹

About 50 years ago, you may have walked up to me… and said: “Hey Frank, are these British Airways cheques? They’re amazing. They look great. But let me ask: do you know where British Airways banks?” I’d have to say that I didn’t know, and that I’d just made up a bank. Today, that’s a phone call away. If I called BA now, and asked to talk to someone in accounts receivables. “Look, I’m getting ready to wire you some funds. I need your wiring instructions.” They’d give me the bank name, account number, routing number … If I hang up and call back to ask for their communications department, I’d ask them to send me a copy of BA’s annual report. Page three has the signature of the CEO, CFO, et cetera. Scan it, digitise it, put it on a cheque.

Criminal fraud may be general, such as theft by false pretense, or specific, like bank fraud, insurance fraud, forgery, and others. For example, in 2019, PointPredictive (pointpredictive.com) estimated that up to $6 billion of US auto loan paperwork may contain misrepresentations, due to synthetic identities, income misrepresentation, phantom loan schemes, straw borrower schemes, and systematic dealer fraud and misrepresentation (McKenna, 2019). Another type of specific fraud is embezzlement, the theft or misappropriation of funds placed in one’s trust or belonging to one’s employer. The majority of embezzlers are first-time...
offenders with clean employment histories; embezzlement is fraud, therefore, in that the fraudster has the “confidence” of their employer and is profiting illegally from their actions. Most embezzlement schemes last about 16 months before they are detected and over half of the victim organizations (most of which are for-profit) never recover any of the fraud-related losses (ACFE Report, 2020). The Association of Certified Fraud Examiners reported in 2020 that over $7 billion in losses were reported and nearly a quarter of the cases reported caused losses in excess of $1 million (ACFE Report, 2020). The fraud triangle is a framework that helps explain why employees commit embezzlement (Figure 1.1). Pressure can be either personal financial pressure, such as living beyond one’s income, or workplace financial pressure, such as a shortfall in revenue. The employee sees the situation as unsolvable by normal, approved solutions and is not in a position to speak with others who may help. The employee thus exploits an opportunity to defraud their organization. The employee identifies a means by which they can abuse their position to resolve the pressure in a way that will not be detected. The employee then rationalizes the embezzlement, justifying the crime to comport with their moral compass. Rationalizations are often based on external ethical factors, such as a need to take care of loved ones or a perceived dishonesty by a supervisor or employer. Although the umbrella term of fraud is used colloquially and specifically by law enforcement, many investigators use “fraud” to mean a specific type of crime, typically fraud against non-governmental organizations. Many textbooks on the topic of fraud approach it this way, meaning forensic accounting, which is only one, albeit important, aspect of fraud investigation.

![Fraud Triangle Diagram](image)

**Figure 1.1** The fraud triangle: pressure, rationalization, and opportunity make up the fraud triangle
The key thing to remember is that for every legitimate business activity, there’s at least one fraud scheme based on it. The fraud may have the trappings or apparent structure of a legitimate business activity, like pyramid schemes, or it may mimic that business activity, as with fake websites for businesses and banks. Frauds leverage a variety of tools and norms in personal psychology, society, economics, and rhetoric. And, as with many things in modern society, the internet and digital life has made fraud easier than ever. Professional fraudsters view the internet as just another tool; con men (and women) were around long before the internet. Many cons have a long history, perhaps as old as civilization. For example, the phrase “to buy a pig in a poke” was first used in 1555 (Heywood, 1555). A poke is a sack (from the French poque, the same word that pockets and pouch come from) and buying a pig in a poke was purchasing something sight unseen. The confidence scam was that the farmer would have substituted the suckling pig for a cat; when the unwary buyer opened his purchase he would “let the cat out of the bag,” meaning to have exposed the scam. The scam may be older than 1555: the phrase appeared in a letter to Martin Luther in May 1530 (Roper, 2016). Con artists understand the core mechanics of a con and update, refresh, and change them to meet the conditions of their times. Technology just makes them faster, easier, and more lucrative to reach more people. The anonymity of the internet means you do not need to face your victim to play out a confidence scam which makes it easier to do and scams can be run from anywhere, many times in a country where law enforcement has no jurisdiction. As might be expected, online fraudsters can be tremendously difficult to trace.

2. OPENINGS

A mother receives a phone call saying her soldier son has been injured overseas. A college student finds the perfect part-time job. A prospective tenant responds to an online classified ad for a great apartment. A man exchanges instant messages with an old college friend who is in trouble. A company creates a miracle weight-loss powder. An office worker returning from lunch finds a lost wallet with $200 in it. These are all openings to scams, each different in their execution but with the same core phases. It is difficult to see a fraudster coming. They don’t fit any single demographic profile. Degrees of deception exist everywhere in our daily lives, complicating our ability to tell truth from fiction. To that end, people expect to be lied to, to some degree, so missteps and white lies are overlooked as misstatements or casual misrepresentations.

No universal taxonomy of fraud exists. Take the following example. At a bar, the person next to you asks you to draw one card from a deck of playing cards and place it face up on the bar for everyone to see; assume the card is the seven of diamonds. The person says she will bet you $5 that her friend, The Wizard, who is not in the room, can tell you which card you chose. She encourages anyone else to go along with the bet. The Wizard can be made available by phone. You agree, thinking there is no way for anyone not in the bar to know what the card is. The woman makes the call, asks, “Is the Wizard there?” She waits a second and then says, “Okay.” In a few more seconds, the woman says, “Hello, Wizard. What’s the card?” and hands the phone to you. The Wizard says, “The card is the seven of diamonds,” and hangs up. You owe the woman $5, along with everyone else that bought into the trick. Magic? Hardly. The woman’s associate, The Wizard, knows what to do. When the woman asks if The Wizard is there, the associate starts saying, “Hearts, clubs, diamonds, spades.” When they get
to “diamonds,” the woman says, “Okay,” and the associate now knows the card is a diamond. To onlookers, it seems like the party on the other end has said, “Just a minute, I’ll get The Wizard.” The associate then starts counting cards up, “One, two, three …” and so on; when they get to the correct card, the woman says, “Hello, Wizard.” She then hands the phone to you, or, better yet, puts The Wizard on speaker for everyone to hear, and the correct card is announced. Is this classic bar bet a scam? Technically, maybe. The woman and her associate did deceive you and the other customers for financial gain; whether it is a crime depends on local laws. Are all bar bets cons, then? Probably not, but they contain the same basic aspects of true confidence schemes.

The taxonomy of cons used in this chapter breaks them into short cons and long cons. A short con is a confidence scheme designed to get the money the mark has on him or can get easily, like from an ATM. The goal of the short con is to get in, get the money, and get gone. The fraudster identifies a likely individual (called the mark) and executes their plan through one or more means, typically through social engineering and observation. For example, you’re in line at the bank. You hear a woman speaking to a man in the line next to yours:

**Woman:** “This line isn’t moving very fast, is it?”

**Man:** “I guess not. You can go in front of me if you like.”

**Woman:** “Oh, gosh, thanks, but that won’t help. It’s my kid’s birthday party and I need to cash this check for his present. He wants to buy his own present. I’m teaching him responsibility.”

**Man:** “That’s great. Sorry about the line.”

**Woman:** [Checks watch] “Wow, I’m going to be late. Can I ask a favor?”

**Man:** “Well …”

**Woman:** “Let me sign the check over to you – it’s only for $150. Do you have that cash on you?”

**Man:** “Uh … yes …”

**Woman:** “Then you could deposit the check into your account and I won’t be late. What do you say?”

**Man:** “That’s a third-party check.”

**Woman:** “Yes, but it’s a check from AmPetCo, a huge company. It’s good. Please? My kid will be so disappointed if you don’t.”

**Man:** “OK. I guess.”

This scenario is based on an actual con: The woman’s check was obviously not good. But why did she choose that man? He was older, well-dressed, and married (his ring was visible), therefore more likely to have children. His age suggested he would feel helpful and protective of women and children. The woman behind the man, who was questioned as a witness, was certainly not the kind of mark the fraudster would approach: She was in her mid-30s, wearing a sharp business suit, and was handling work communications over her mobile phone. People constantly communicate about who they are, intentionally or not. Expressions of affiliation are broadcast on t-shirts (LAKE CITY COLLEGE), details about our lives by blabbing on cell phones, chatting amiable at a smokers’ corner outside an office (Is that the new hire or a stranger?). What can you tell about somebody from their car? College affiliations, children’s schools, political affiliations, expired tags, and more. Social media, like Facebook, Twitter, Instagram, and other platforms, allow people to essentially firehose personal information to
the world. The grandparent’s scam, for example, is a modern take on using personal information. The phone rings, the caller ID says it’s the police department, so the person answers. “The police” tell you they arrested your grandson, giving his correct name, for driving while intoxicated. They tell you the make and model of car he was driving and the name of his passenger, his girlfriend. The grandparent knows this information and it is accurate. This must be the police department: How could anybody else have all that information? Therefore, when the request is made to wire bail money to get the grandson out of jail, it seems real and reasonable. All that information (and more), however, is easily available on social media; spoofing a caller ID is a relatively easy matter. The money is wired and the fraudsters evaporate. Our desires to communicate about ourselves make it easy for fraudsters to find an in, a way to approach them socially and gain a moment’s trust to execute a short con.

By contrast, a long con is a scam that unfolds over several days, weeks, or even years and may involve a team of confidants, as well as props, sets, extras, costumes, and scripted lines. The goal of a long con is to relieve the victim of huge sums of money or valuable things, often by getting him or her to empty out banking accounts, borrow from family members, and otherwise leverage their finances to invest in the con. Long cons take many forms and only a few of the classics are described here. The Big Store is a long con where an environment is created in which to run the scam completely under the fraudster’s control. Everyone in the environment, except for the victim, is involved in the scam (historically called shills, they are confederates of the fraudster and are in on the con). For example, in 2014, a rural co-operative in Nanjing, China constructed an entire brick-and-mortar fake bank with uniformed clerks behind counters. The unlicensed bank operated for a little over a year, then defaulted on its obligations, swindling its “customers” of 200 million Chinese yuan (about US$32,000,000).

A classic long con is The Wire, where a mark is lured into wagering on rigged off-track betting by promising advance knowledge of the outcome of a race. The person who lures the mark, called the roper, makes promises of advance knowledge and guaranteed wins. The movie The Sting is a textbook example of The Wire. Most popular in the early twentieth century, The Wire worked because race results were sent via the telegraph to betting establishments. A telegraph operator could delay racing results long enough for a few shills to place bets and make good money off the marks. The Wire takes time and requires a team of shills to set up and operate what appears to be a staffed betting parlor. Today, with the digital wonders of the internet, The Wire is an even easier con to run, because the requirements for perceived legitimacy are lower. In a twist, The Payoff is a long con where a wealthy mark believes he has been taken into a deal – that is, he or she thinks they are a shill – to swindle a large syndicate of some type, like racing or drugs. The mark is first given money by the fraudsters to bet as a front and is later “put on the send” to get as much of the mark’s own money as possible to bet. The mark, of course, loses big.

The Rag has the same structure as The Wire but it is done with stocks instead of off-track betting. Invented in the 1920s, “investing” in stocks at the time was much the same as betting on a horse, yielding a potential quick turnaround. Today’s digital currency initial coin offerings (ICOs) are a potential venue for a refreshed version of The Rag. Unlike initial public offerings (IPOs), investing in an ICO does not result in an ownership stake of the company: It is basically a bet that the unmoored, currently worthless digital currency purchased now will increase in worth later and yield a profit. For example, members of Reddit’s WallStreetBets forum were targeted in May 2021 in a likely cryptocurrency scam that could have left its victims with at least $2 million in losses (Kochkodin, 2021).
Whether short or long, all scams require a good story, a vulnerable mark, a means of cashing out, and scalability. In modern terms, a “vulnerable mark” can also be poor internet security, lack of security protocols on a facility, bad information handling, and ease of human engineering.

3. THE NARRATIVE

People who say they don’t click on suspicious emails present themselves as being savvy about fraud. These same people, however, will post pictures of family and friends and activities and work related activities on social media, including answering surveys on platforms that provide personal information that could be used to circumvent Knowledge-Based Authentication (KBA). Static KBA is a website asking for your mother’s maiden name; a dynamic one is when the website asks which of the following cities have you lived in. The dynamic list is generated real-time by a service. While posting common static KBA information is unwise, it seems less harmful to say one lived in Poughkeepsie, New York. And while people may feel a bit more secure filling in the Captcha box, there are algorithmic systems that can defeat Captchas as well as “Captcha farms,” which are sweatshops where humans are paid very small amounts of money (as low as $1 per thousand) to solve reams of Captchas (Motoyama et al., 2010). Technology, therefore, is one of the weaker links in fraud prevention. The human target, the mark, is the last but most relevant line of defense against fraud. To shore up and strengthen this bastion of prevention, it is necessary to understand why people fall for cons in the first place.

A Con is a Story

Storytelling is narrative communication, a sequencing of events told to others. Humans have a “narrative hub” in the brain, a network of various parts of the cerebral cortex which allows the inference of thoughts, feelings, and motivations of others based upon their actions and words. During a story, the listener projects themselves into the thoughts and feelings of the main characters, letting them think and feel what they believe that character thinks and feels (Yuan et al., 2018). Humans are literally hardwired for narratives. This is central to a con because narratives are inherently persuasive (Dahlstrom, 2014).

Every story ever told has the same core structure in three acts: (1) Set-up or the problem, (2) the confrontation or the journey, and (3) resolution or solution. The basic structure of narratives can most easily be seen in jokes, a very old type of narrative. The following is the first known recorded joke from The Laughter Lover written by Hierocles and Philagrius in the third or fourth century AD:

A barber, a bald man, and an absent-minded professor take a journey together. They have to camp overnight, so decide to take turns watching the luggage. When it’s the barber’s turn, he gets bored, so amuses himself by shaving the head of the professor. When the professor is woken up for his shift, he feels his head, and says, “How stupid is that barber? He woke up the bald man instead of me.” (West, 2016)

A simpler example is a shorter “classic”:
Hook, line, and sinker: the mechanics of fraud

… a guy walks into a psychiatrist’s office and says, hey doc, my brother’s crazy! He thinks he’s a chicken. Then the doc says, why don’t you turn him in? Then the guy says, I would but I need the eggs. (Allen et al., 1977)

Using the simpler joke, the structure becomes evident:

1. First act (set up): a guy walks into a psychiatrist’s office and says, hey doc, my brother’s crazy! He thinks he’s a chicken.
2. Second act (conflict): Then the doc says, why don’t you turn him in?
3. Third act (resolution): Then the guy says, I would but I need the eggs.

In Act 1, the characters and their environment are established. Act 1 must also engage the audience with an exciting scene early on that grabs interest and keeps them intrigued as to what happens next. The engagement should provoke a change in the audience and give them a novel experience that challenges or encourages them. In the chicken joke, the man with the mentally ill brother addresses the psychiatrist in the professional setting of the psychiatrist’s office with the startling statement about his sibling’s welfare. In Act 2, the audience then leaves their comfort zone and seeks a goal to the problem described in Act 1.

The stakes tend to escalate: Why hasn’t the brother institutionalized his brother? This escalation pushes the narrative into a moment of crisis: The brother must either act or remain in the situation he sought to alleviate by coming to the psychiatrist in the first place. Finally, Act 3 resolves the confrontation with a conclusion and solution to the problem created in Act 2: The brother needs the eggs. After Act 3, there may be a denouement, where the strands of the narrative are drawn together with explanation. In the chicken joke there is none, leaving one to wonder where the eggs come from or if mental illness runs in the man’s family.

Read the following example of a con, developed by the Australian Competitive and Consumer Commission, and look for the narrative structure.

Davin received a private message on Facebook from the ‘Facebook Freedom Lottery’ claiming he and others had won amounts up to $150,000. At first he didn’t believe it. Businesses don’t give money away out of the blue and to win in a lottery you need to buy a ticket. However, moments later his cousin who he hadn’t spoken to in some time sent him a Facebook message about the winnings. His cousin claimed that he had also won and noticed Davin’s name on the list of winners. He claimed he had already received his winnings after going through a relatively easy process.

Trusting his cousin, Davin began the process for accepting the prize money which required him to first pay a small upfront fee of $250. Once this was paid, he was to receive the money into his nominated bank account for which he provided details. The next day he was informed that since the prize money was sitting in a bank in Germany, he would have to pay an ‘international transfer fee’ which could not be subtracted from the winnings for some complex legal reason. Davin reasoned that since his cousin had managed to receive the money, then he must have gone through the same process and so he would also pay this additional fee.

Over the next two weeks, Davin paid five more fees, each time believing it would be the last. Eventually, in desperation, he spoke to his cousin and asked how many fees he paid before he received his winnings. Davin’s cousin had no idea what he was talking about and told him that he had only just regained control of his Facebook account after it had been hacked.

It then became clear to Davin that he had been scammed. There never was any prize money and the Facebook message was part of the scam. By this time, Davin had already sent $1500 and handed over a wealth of personal information to scammers.
What’s the three-act story in the pitch made to Davin?

1. You’ve won the lottery.
2. You have to make a payment (and more payments) to transfer funds.
3. Once you do, you’ll get the money.

Narratives are the quickest path to emotion, drawing on two mental shortcuts, the Affect Heuristic, where people make decisions based on whether they feel something is “good” or “bad” without conscious analysis, and the Affect Pool, where listeners to a narrative draw from previous feelings similar to those offered in the story (Kahneman, 2011). Humans’ affinity for narratives, drawing on the Affect Heuristic and Affect Pool, set them up unwittingly for con schemes.

4. THE ELEMENTS OF A CON

As previously stated, all cons have the same basic forms, like any narrative. How many steps make up a con varies, however. The classic series of steps, offered by Mauer (1968) are:

- **The Put-up**: Choosing the mark
- **The Play**: Establishes trust with the mark through storytelling
- **The Rope**: Making the pitch
- **The Tale**: Showing how the mark will benefit
- **The Conviner**: Letting the mark win
- **The Breakdown**: Seeing how far the mark will go
- **The Send**: The mark goes to get more money
- **The Touch**: Taking the mark’s money
- **The Blow-off and The Fix**: Get away fast before the mark realizes; bribing the police

Not all cons, even long cons, have each of these steps explicitly, however. A simpler description is offered by Wilson (2020) and has the benefit of using a common phrase as a mnemonic:

- **The Hook**: Get them interested in the bait
- **The Line**: Build their desire, sell the story, and establish rapport
- **The Sinker**: Close the deal
- **The Blow-off/Cool-out**: Get away with the money; have the mark quietly accept their losses

This structure patterns well with the known aspects needed for fraud to occur:

- Vulnerability: The Hook
- Deception: The Line
- Belief: The Sinker
- Embarrassment: The Cool-out

And the narrative structure discussed previously:

- Act 1: The Hook (Set-up)
- Act 2: The Line (Confrontation)
To recognize the components of a scam as a specialized type of narrative, and thus the scam itself, each of the component steps will be discussed in detail.

**The Hook**

To recognize the components of a scam as a specialized type of narrative, and thus the scam itself, each of the component steps will be discussed in detail.

**The Hook**

The most important element of the hook is the bait: Every trap requires bait. Typically, the bait is money but could be other human desires, such as lust, love, revenge, and the other staples of human criminal activity. If the fraudster knows what the mark wants or desires, they can take everything the mark has. Relating to Maslow’s Hierarchy of Needs, some needs take precedence over others, with the more basic, primal ones being lower on the hierarchy (Figure 1.2). Frauds take various forms on how to deploy the bait. Some scams require the bait to be cast and then wait for a bite, like casting a wide net and waiting to see what’s caught. Many, however, introduce the bait in a way that dictates the mark’s perceptions for the rest of the con. This starts what is known as the bubble, the altered perceptual reality that envelopes the mark’s thinking about the con. Because the bubble keeps the mark in the con, The Hook is crucial to a successful con.

**Figure 1.2**  
Maslow’s (1954) hierarchy of needs

Three types of hooks are recognized: Big, Soft, and Straight. A Big Hook is set for anyone to bite. They are thrown at the largest audience that can be found and someone eventually will bite. Connecting the mark to the bait is therefore a numbers game. Many cons run on the internet use Big Hooks: If one million scam emails are sent (“You’ve won the Irish Sweepstakes!”), 99 percent of recipients might not fall for it but the remaining 1 percent who do still means 10,000 marks to work on.

A Soft Hook uses subtlety, like an overheard conversation or phone call in a cafe, for example. The objective is to have the marks chase the bait themselves, in essence, and it is very effective to have the mark believe they are in control; this reinforces the Bubble. Also known as an Open Hook, it is bait the mark takes willingly. For example, the fraudster speaking over a mobile phone in a cafe says she just found a nearby flea market stall selling a “Hollingworth Blueware” plate, which the fraudster says is worth thousands, for a ridiculously cheap price, say $100. The fraudster says they do not have the funds on them right now but gives their “friend” on the other end of the phone directions to the cafe and tells them to bring some money. The fraudster then sits down and gets a cup of coffee. With luck, some sharp-eared mark in the cafe will take the Soft Hook and go to the flea market to buy what they think is an investment bargain. “Hollingworth Blueware” plates do not exist; they are cheap plates bought in bulk and stamped with a fabricated logo on the bottom to suggest legitimacy. The flea market stall worker is a shill, says little, sells the plate, and replaces them after sale, waiting for the next mark.

Finally, the Straight Hook quickly comes down to “yes” or “no.” It is a favorite of “walk-up scammers,” like the woman with the third-party check in the bank line. A staple of “hit-and-run” scams, the Straight Hook must be immediately engaging. For example, in the Pigeon Drop, it depends on encouraging the mark to hold onto something of value in return for a good faith deposit that proves he will split a sum of money when the time comes. The key is to create a reason not to split the money at that moment. Using a simple example of a Pigeon Drop with a Straight Hook, the four components of a con will be detailed in the following sections.

A man emerges from the bathroom of a bar with a gold necklace in his hand, and engages the mark, saying he found it on the bathroom floor and admiring how shiny and expensive it looks (the Straight Hook). The mark is hooked with the found necklace and the value it suggests.

Now comes the line.

The Line

The bar phone rings at that moment. The bartender answers it, chats a second, and then asks the patrons if anyone found a gold necklace; the man on the phone bought it for his wife, thinks he lost it here, and offers a $200 reward for it. The fraudster with the necklace says, “We’ve got it here,” bringing the mark into the fold. The bartender speaks to the man on the phone, hangs up, and says the necklace owner will arrive in 30 minutes. The man who found the necklace tells the mark he is running late and can’t wait 30 minutes for the owner to arrive. Then the man tells the mark he has an idea.

The Line adds layers to the story, deepening it while making it both enticing and believable. The longer the mark is on The Hook, the more likely they are to become suspicious or lose their nerve. The Line gets the mark more involved at each step, therefore being more likely to trust the scam and possibly to increase the stakes.
One of the most powerful aspects of a great con is that it often uses the truth (or some portion of it) to support a lie. Most advertising sounds something like this: Maxima’s ‘Mazing Weight Loss Juice, when used with a balanced diet and exercise, can help you melt away fat! The truth is, diet and exercise will do that anyway: The juice could be just about anything that was not too caloric. Another strong strategy is for the fraudster to provide the mark with a bit of information but then have him receive the same information through another source, such as internet links, email, conversation, or other “independent” means. The mark decides that separate sources must be true, thus strengthening The Line. The principal objectives of The Line are to satisfy the mark’s concerns, feed him information, control his options, manipulate his perceptions, and give him confidence in the scenario.

The reason the mark’s options need to be controlled is that a con is a warped reality. The con artist creates a bubble of “alternate reality” around the mark. The longer a con goes on, the mark may wise up. Friends and family, not privy to the con’s Line that created the bubble, might talk the mark out of the deal. The bubble isolates the mark in a number of ways. The mark may be isolated physically, although this is difficult to do. Typically, though, the fraudster creates reasons for the mark not to talk about the “deal” with others, whether that it’s criminal activity, secrets that should not be shared lest others try to barge in on the deal, inside information that will get someone in trouble, or similar contrivances. Remember, cons are about altering the perceived choices of the mark: “That’s what THEY want you to think. WE know what’s really going on.” Contrived confirmation bias holds them close. Inside the scam’s bubble, there is hope and opportunity; outside is only doubt and fear. If the fraudster has done their job, the bubble can only be burst from the inside (the last component). The fraudster will have anticipated conflicting information and has plans to address it ahead of time to control the mark’s perceived options.

The Sinker

The man makes the mark an offer: They split the reward. If the mark gives him $100, he will give him the necklace, and the mark can get his money back when the owner arrives. The mark agrees and sits down with a drink to wait for the necklace’s owner to arrive.

Arguably, the most critical and delicate point in the scam is where the mark hands over the money or valuables, called The Sinker. The Sinker can be either contrived or unfold naturally; regardless, the fraudster typically creates an imperative that forces the mark to make a decision, such as time pressure or an outside force. A different approach is to let the mark think they are taking over; let them push for closure, giving them the illusion of control. If The Line is about securing trust, The Sinker is about securing commitment. Money in hand, the fraudster needs to now leave as soon as possible without creating suspicion.

The Cool-Out/Blow-off

The “owner” of the necklace never shows up. The necklace is sparkly but worthless and the mark is out $100.

Why would fraud be under-reported? The shame, guilt, embarrassment, and disbelief of the mark having been conned all contribute to a lack of reporting fraud. When a mark is too embarrassed to report the fraud to the police, that is a Cool-out. The bubble helps the Cool-out: The fewer people that know what the mark has been up to, the easier it is for the mark to conceal
it. When the victims doubt their own judgment or refuse to believe they’ve been conned, the fraudster can walk away cleanly; that is a Blow-off. Overall, however, the mark is generally afraid about how their family members, friends, and business associates will react. Some feel their losses are not large enough to report, do not want to get involved in the reporting, or think law enforcement agencies will not take the crime seriously. Most victims feel they only have themselves to blame, when in reality, calculating, skilled perpetrators are to blame for these criminal acts.

5. PSYCHOLOGY OF FRAUD

The Nobel-prize winner Daniel Kahneman describes two different ways the brain forms thoughts, what he calls System 1 and System 2 (Kahneman, 2011). System 1 is fast, automatic, always “on,” emotional, stereotypic, and subconscious; it is intuitive, powerful, impatient, and impulsive. While it works on many issues and levels at the same time, it uses little energy, quickly creates meaning out of sometimes very little, and is easily influenced. System 1 will believe almost anything. By contrast, System 2 is slow, effortful, infrequent, logical, calculating, and conscious. It is rational, methodical, and cautious; with little processing power and limited capacity, it becomes singularly focused. System 2 is a slow, heavy energy user. System 2 can override System 1 under normal conditions. But if System 1 is highly agitated or emotional or System 2 is tired or preoccupied, then System 2 fails to be able to control System 1. Although System 2 is very good at making comparisons, it does not perform well under pressure.

Based on these descriptions, it would seem like one should engage System 2 for every decision but System 2 is not always right. Think of a class of students taking a math test: They are all making System 2 decisions but the number of right answers will vary from student to student. Also, if their teacher has given them bad information, their answers will be bad, also. And it may seem like System 1 is a bad process to rely on for making important decisions. But the mental models and short-cuts System 1 uses for parsing the world are necessary for people to process what otherwise would be a bewildering torrent of information. People’s cognitive load would be too high to process the world in a timely fashion. These models or short-cuts, called heuristics, allow people to be mostly right about most things most of the time. Heuristics have served an adaptive evolutionary purpose, keeping humans alive for millions of years. Consider a human ancestor on the savanna who hears rustling in the grass. System 1 says, RUN. If you do and it’s your friend playing a practical joke on you, you live to laugh about it; if you don’t, say by using System 2 to reason it out, and it is a lion, then you die. System 1 can be a life saver.

People are not rational. People are cognitively biased. Relying on heuristics is all well and good but humans are very susceptible to biased thinking and the heuristics may use those biases or feed into them, making rational thought murky or very difficult. These cognitive biases are the evil twin, so to speak, of useful heuristics that easily derail System 2. A cognitive bias refers to a systematic pattern of deviation from rationality in judgment. The problem is biases happen unconsciously. Cognitive biases are like optical illusions of thinking: It takes effort to see “through” them. Some of the cognitive biases that are exploited in cons are described below.
The availability bias makes something seem more likely or have greater consequences if it is easily recalled. People tend to heavily weigh their judgments toward more recent information, making new opinions biased toward that latest news. But the frequencies at which events come to mind may not be accurate reflections of the probabilities of such events in real life. Think of this: What would be considered more likely: Being killed by a shark or by parts falling off an airplane and hitting someone? Sharks are everywhere, shark attacks are reported regularly, and there are even entire weeks of programming dedicated to sharks. Who has ever heard of someone dying by having an airplane part fall on them? This is the availability bias at work: All that shark media coverage belies the fact that a person is 30 times more likely to die from falling airplane parts than by a shark attack (the risk of a shark attack is one in 300 million, being hit by parts from a plane is one in only 10 million).4

Anchoring is the tendency to rely too heavily on, or “anchor,” one trait or piece of information when making decisions. Once an anchor is set, other judgments are made by adjusting away from that anchor, and there is a bias toward interpreting other information around the anchor. JCPenney thought it was a smart move to eliminate coupons and instead create “everyday low pricing.” Sales plummeted. The company had not realized how influenced customers were by thinking they were paying not $29.99 for a product but they were getting a bargain at the marked-down price of $19.99 – they thought they were saving $10 off the retail price. The company reversed their policy and customers returned.5 The customers needed to see the anchor price to inform them that they were getting a bargain.

Confirmation bias is cherry-picking information that confirms existing beliefs or ideas, rather than actively seeking information to refute them. It is the tendency to search for, interpret, favor, and recall information in a way that confirms one’s preexisting beliefs or hypotheses, while giving disproportionately less consideration to alternative possibilities. People display this bias when they gather or remember information selectively, or when they interpret it in a biased way. One way to think of confirmation bias is as an absence of active open-mindedness. As a demonstration of confirmation bias, show a group of people this sequence of numbers: 2, 4, 6. Next, have them offer examples of number sequences that they think demonstrate the rule and tell them if it conforms to the rule; do not let them state what they think the rule is. Most people will offer examples like 8, 10, 12, or 1, 3, 5. After a few examples, they should be confused because the rule is “any three increasing numbers, so 1, 5, 189 conforms to the rule, as does −1, 0, 1. What most people will not do is offer examples that violate what they think the rule is; that is, they will not systematically test if they are wrong or not, but keep trying to validate what they think the rule already is. Confirmation bias is stronger for emotionally charged issues and for deeply entrenched beliefs. People also tend to interpret ambiguous evidence as supporting their existing position or stereotype: If a new Canadian friend hates hockey and loves sailing but a new Mexican friend hates spicy foods and loves rap music, the new stereotype-inconsistent information is less likely to be remembered (Sanderson, 2010). Persons believing in extrasensory perception (ESP) will keep close track of instances when they were thinking about someone, say their mother, and then the phone rang and it was her, yet they ignore the far more numerous times when they were thinking about their mother and she didn’t call or when they weren’t thinking about their mother and she did call. They also fail to recognize that if they talk to their mother about every two weeks, their frequency of “thinking about Mom” will increase near the end of the two-week interval, thereby increasing the frequency of a “hit.” The internet has perhaps honed confirmation bias
to a new level of ease: If the initial search fails to turn up the results desired, the search terms are easily adjusted until they do.

Whenever possible, people try to avoid losses of any kind, and when comparing losses to gains they don’t treat them equally. This is called the sunk cost bias. Although people think they make rational decisions based on the future value of objects, investments, and experiences, their decisions are tainted by the emotional investments that they accumulate, and the more something is invested in, the harder it becomes to abandon it. The person who hated the first 30 minutes of a movie but sat through the last hour and 30 minutes of it because “the tickets were expensive” is suffering sunk cost bias. When factoring the costs of any exchange, people tend to focus more on what they may lose in the bargain than on what they stand to gain. Studies show non-human animals and small children do not commit this fallacy. Wasps, worms, rats, raccoons, and toddlers do not care how much they’ve invested or how much goes to waste. They can only see immediate losses and gains (Arkes and Ayton, 1999). In one experiment, a booth was set up where passersby could purchase chocolates—a Hershey’s Kiss for one penny or a Lindt Truffle for 15 cents. The majority of people who faced this offer chose the truffles. Later, another booth had the same two choices but lowered the price by one cent each, thus making the kisses free and the truffles 14 cents each. This time, the vast majority of people selected the kisses instead of the truffles. If people acted on pure mathematical logic, there should have been no change in the behavior of the subjects: The price difference was the same. But people do not think that way and their loss aversion system is always vigilant, waiting on standby to keep them from giving up more than they think they can afford to spare (Ariely and Jones, 2010). Think of it this way: Every garage sale is a funeral for someone else’s sunk costs.6

Belief Bias is when people accept things that fit in with their belief systems and reject things that do not. In other words, if people agree with a viewpoint, they are inclined to believe that the process used to obtain the results must also be correct. The reverse is also true: people will tend to reject assertions that do not fit in with their belief systems, even though these statements may be perfectly logical and arguably possible. In relation to fraud, if people believe “you can’t win if you don’t play,” they typically will be more willing to be hooked by lottery-like schemes, among others.

Finally, the clustering illusion, also called the “Hot Hand Fallacy,” is the tendency to overestimate the importance of small runs, streaks, or clusters in large samples of random data (that is, seeing phantom patterns, a type of mental pareidolia, the literal seeing of pattern or forms that do not exist—like a face in the clouds—which is a natural human trait, probably linked to System 1). When a person’s streak of successes fails to meet their stereotype of a random sequence, it is concluded that person has a “hot hand,” and is experiencing a streak of luck. People, in general, are very poor statistical thinkers. Assume a quarter was flipped 10 times with these results (heads or tails): H, T, H, T, H, H, H, H, H, H. Is it a fair coin? That may seem like a “lot” of heads but over 10 flips with a fair coin, it is a possible outcome. Remember, one toss of the coin has nothing to do with the next. If the coin was flipped 100 times and heads came up 80 percent of the time, then there would be cause to worry. This is the small number fallacy, where a faulty generalization is reached based on insufficient evidence. Most modern roulette wheels in casinos have an electronic display that shows the last ten spins. Gamblers will scrutinize this information to count how many red and black numbers have come up, hoping they will predict the next spin. On a fair wheel, each spin is independent, like the coin, so these numbers do not help at all, but the gamblers think they do.
Why are stories so important to humans and their interactions? Why do these biases work? A short exploration of human psychology and how we interact with each other will help to answer these questions. You offer to buy a stranger a soft drink and they accept. If you then ask them to buy $5 worth of raffle tickets for your child’s after-school club, they are far more likely to buy the tickets than if you had not purchased the soft drink for them. This rule of reciprocity (Cialdini, 2021) works even when, like the soft drink and raffle tickets example, the value of the gift is far less (1/10th in that example) than the value of what is later asked for. People feel obligated to reciprocate generosity in the future with repayment through favors, gifts, invitations, and other methods. Living with knowing that “if I scratch your back, you’ll scratch mine,” people can initiate an exchange or relationship without the fear of loss. This has been important in the evolutionary history of humans: It creates a web of indebtedness that allows for the division of labor, exchange of diverse forms of goods and services, and creates interdependencies that bind individuals into effective units. By lowering the cost (risk) of transactions, a sophisticated and coordinated systems of aid, gift giving, defense, and trade became possible with enormous benefits and advantages to societies. On the down side, this extremely powerful rule leads people to say “yes” to things they never would except for the indebtedness. The rule of reciprocity puts the power in the hands of others: Individuals do not choose to receive this debt. Marketers and advertisers know this and, therefore, free samples, discounts, dinners, and other gifts pull us into situations that might otherwise be avoided.

In another example, researchers pretending to be vacationing placed a blanket, radio, and personal things close to a person who was not involved in the research. After several minutes, the researcher would leave. A few minutes later, another researcher playing the role of a thief walks up and takes the radio. In these circumstances, only 4 out of 20 people tried to stop the thief. In repeat experiments when the onlooker was asked, “Watch my things?” before the researcher left, 19 out of 20 tried to stop the thief (Moriarty, 1975). Once a person’s self-image is established (“I’m helpful. I stopped a theft”), that person should comply naturally with a whole range of requests that are consistent with this new self-view.

Related to reciprocity is the reject-then-retreat technique. A large request is made, one that will most likely be turned down. Then, after the refusal, a smaller request is made that now seems reasonable in light of the first number (which plays off the bias of anchoring, discussed earlier); the subsequent request was the intended goal and the larger request was a feint to get to it. The reject-then-retreat technique uses the pressure for reciprocation to increase compliance. By rejecting the first offer, the target now feels obligated to accept the next one. A common form of this technique can be seen in strong sales pitches, like:

- Would you pay the $39.99 retail price for this product? [No]
- Of course not. How about $29.99? [No]
- Then $19.99 and I’ll throw in a free one? […] Yes […]

By reject-then-retreating and then offering a gift (the second free product), the mark now feels obligated to accept, whether they want the product or not. The $19.99 price was the intended goal all along, based on what the product cost the seller to buy or make.

Another powerful influencer is the mere exposure effect, where simply by having seen something previously makes a person more positively oriented toward it. In one study, a researcher showed people images of a range of items, some of which they could not comprehend (they were nonsense words in Turkish) and then tested their liking for them. Consistently, people chose the shapes they had seen previously as more pleasing even though they had no
idea what they were (Zajonc, 2001). The mere exposure effect has evolutionary value: If something has been seen before, and it was not harmful, then it is at least benign ("better the devil you know"). This works for people as well. According to a study by Robin Dunbar at the University of Liverpool, primate brain size is determined by social group size. Dunbar’s conclusion was that most human brains can really understand only an average of 150 individuals as fully developed, complex people (Dunbar, 2012). According to researchers, tribalism is in some sense an inescapable fact of human neurology simply because many human brains are not adapted to working with large populations and the tendency is to favor those we know, like family and friends (Tong and von Hippel, 2020). Once a person’s limit for connection is reached, the human brain must resort to some combination of hierarchical schemes, stereotypes, and other simplified models to understand so many people. What is interesting for fraud purposes is that the amount of time primates, including humans, spend in physical grooming behaviors to create social bonds and resolve conflicts is about 20 percent. However, for non-human primates, the maximum group size is around 80, almost half of humans’ maximum group size number. So, how can humans deal with so many more social interactions? It is argued that language is a proxy for physical grooming (Dunbar et al., 1997). Language allows people to establish their reputation, share news about others which establishes their reputations; reputations are a short-cut to knowing someone. Thus, reputation and sense of self is what makes many facets of a fraud scheme work:

- The Hook: How the fraudster presents themselves, seemingly reputable or at least benign (hence “confidence schemes”).
- The Line: Narratives and stories engage people, placing them in a social position that flatters them (“I’m only telling this to you because you’re the kind of person who will appreciate it …”).
- The Sinker: Marks have made a bargain with the fraudster and feel compelled to keep it.
- The Cool-out/Blow-off: People want others to think well of them, so they keep quiet about being scammed.

The next section will explore some examples of fraud from a range of old school and new takes on core schemes.

6. EXAMPLES OF FRAUD

Originating with mail order brides and printed ads or catalogs filled with apparently lonely foreign women, romance fraudsters now create fake profiles on dating sites and social apps, striking up a relationship with the mark to build trust; the interactions start slowly then build to more intense and frequent communications (through chat functions). Over time, the mark is groomed to believe they are in a real relationship. The mark’s emotions are manipulated and directed towards the fraudster’s goal, which is usually money but can ultimately be anything. The internet has greatly enhanced these scams with chat rooms and texting using images of someone other than the fraudster as bait. Catfishing is a type of deceptive activity where a person creates a sock puppet account (an online identity used for purposes of deception).\(^8\) Using the sock puppet account, the fraudster baits the mark with images, messages, and content to hook them. The fraudster will offer some situation where they are remote and working in a difficult or exciting field, like working on an oil rig, in the military, or a medical
professional doing humanitarian work. The fraudster then offers a story about needing money. The request may be to pay for a plane ticket or travel, surgery or other medical expenses, customs fees to retrieve something that’s needed, pay for a visa or other official travel documents, tuition for graduation, or even bribes to secure their release from controlling family members. This leads to further requests for more money due to complications while deepening the fake relationship. Romance scams are often carried out by organized criminal networks, who work in conjunction to take money from multiple marks at a time. Fraudulent acts may involve access to the victims’ money, bank accounts, credit cards, passports, email accounts, or national identification numbers or by getting the victims to commit financial fraud on their behalf. Romance scams fleeced a record $304 million from lonely marks in 2020.9 Romance scams are now automated via websites and dating apps, where algorithms complete the chats with little human intervention. One vendor of a software package guarantees a 1.2 percent response rate.10

Real secret shoppers exist. These are people whose job it is to shop in stores, check customer service, and to surreptitiously evaluate a store’s performance. Secret Shopper Scams take advantage of people who may be looking for additional income to make ends meet. The fraudster asks the mark to do one or more of the following:

- to pay a registration fee to become a secret shopper (which does not happen);
- purchase goods or services and then send them to a location for review (never to be seen again) with a promise for reimbursement;
- receive a check (say $3,300) and test the quality of a money transfer (“wire”) service by depositing it and wiring the agreed sum, less the mark’s pay for evaluating the service (say $400).

The first two are straightforward. The third takes advantage of banks’ processing times. The check sent to the mark ($3,300) bounces after it is deposited but this is not known immediately because, while it usually takes about two business days for a deposited check to clear, it takes about five business days for the bank to receive the funds. The mark then ends up being liable for the $3,300. Additionally, the mark may have provided their bank information and now the fraudster has access to the mark’s accounts. Once the money is wired, it is gone. Secret Shopper scams exist in a variety of forms, like mail forwarding businesses, drop spots (“Work From Home! Just forward these packages to …”), offers of easy to exchange merchandise, gift cards, and so on. Entire ecosystems of fraudsters and computer networks may be involved in the larger schemes. An advance fee scheme is when a mark pays money to a fraudster in anticipation of receiving something of greater value, such as money, investments, gifts, or similar, and then receives little or nothing in return.

The mail forwarding scam is similar to the reshipping scam. Advertisements offer jobs involving the forwarding of monies or goods collected in the US to business entities in other countries. The successful applicants will allegedly make thousands of dollars through working from home for a few hours a week, with no special skills or training required. “Avoiding transfer fees” and other complicated excuses will be made. The mark will process payments through bank or payment accounts, supposedly retaining some percentage and wiring the remainder to the “employer.” The payments are described as being for online auctions (where no goods were delivered), forwarding products to overseas customers to avoid duty or taxes, or similar excuses. The products in question are either stolen or obtained through
card-not-present (CNP) charges (entering the card data on a website, for example). The scam can be run in reverse. For example:

- If a person lists a car or motorcycle for sale, they may get an overseas buyer, who “mistakenly” sends too large a check and wants the mark to forward the rest to Company X for shipping costs.
- In response to a rental inquiry, the person sends too large a check, perhaps citing it is their scholarship award and the check can’t be split because the fees are too high in their country or currency exchange problems will be cited.
- Or it’s a refund check for a failed sale for something that would have cost more; it would take 30 days to clear a check from Country X, so they need to have an American third party send the payment.

The patterns are the same but the narratives vary by the mark that is targeted. Why is the mark responsible after being scammed? The US Federal Deposit Insurance Corp (FDIC) requires banks to make money from cashier’s, certified, or teller’s checks available within five days. Consequently, funds from checks that might not be good are often released into payees’ accounts or handed to them in cash long before the checks have been honored by their issuing banks. High quality forgeries can be bounced back and forth between banks for weeks before anyone catches on to their being worthless, by which time victims have long since turned over the monies the bank gave them to the con artists. And, not for nothing, the mark may have shipped stolen goods.

7. FRAUD CONTROL STRATEGIES AND CONCLUSIONS

Broad strategies for employers (the “crime at work” category in this volume) to prevent fraud are straightforward but require commitment and vigilance. First, employers need to know their employees. Fraudsters often have behaviors that can flag their intention to commit fraud. Changes in attitude may be a strong indicator of potential attempts to commit fraud at work. Missed promotions, additional assignments, personal or family problems, or friction with other employees may provide rationale for seeking financial revenge. Creating and publicizing a fraud reporting system is a key strategy to prevent fraud. It is a signal to all employees that management is aware of fraud and will be monitoring for offenses. Additionally, more than half of workplace fraud is caught through the use of anonymous tip lines, making it an inexpensive but effective deterrent (ACFE, 2020). Internal or process controls are a good way to maintain financial safety against fraud. Segregating duties is a significant component of fraud deterrent; this makes it difficult for one person to have access to and authority over company funds. For example, the person who writes the checks for payments should not be the signatory. In smaller companies this may be difficult but third-party companies and software can make this possible. Documentation is another important internal control. Records of credits, debits, sales, and other transactions should be available for audit purposes. Consecutively numbered pages, checks, and other documents help to prevent “paper loss.” New vendors should be scrutinized, as fraudsters have created false companies for payouts typically sent to a post office box. At least annual reviews of vendors and internal controls should be implemented. An overlooked but important strategy for detecting fraud is to monitor vacation balances. Employees who take little or no vacation may in fact be afraid of what would be
discovered should they be gone for a week or two. Duty rotation or spot audits by supervisors or third parties can help avoid this deception. Just as companies need to know their employees, they also need to know who they hire as outside consultants or auditors. Vetting these experts is crucial, because they will have access to the company’s sensitive financial information. There should be no conflicts of interest, such as hiring an employee’s friend or relative, for this type of job. Finally, a positive work environment can deter fraud, as well as being an excellent overall corporate strategy. Open-door policies can help employees feel like they can bring concerns to managers. Likewise, managers and supervisors should lead by example, promoting ethical behavior as the core values of the organization.

As a crime-as-work, financial crimes vary from basic theft or fraud committed by individuals to broader operations run by organized criminals, many of which are multinational. These organized operations are serious criminal enterprises engaging in a broad range of crimes that are often closely linked to violent crime and even terrorism. Criminal gangs operate transnationally to avoid detection and prosecution with ill-gotten funds crossing many physical and virtual borders. Corruption and gambling, particularly in sports, are a common source of international crime and corruption. For example, to date, seven Interpol operations have resulted in more than 30,000 arrests, the seizure of some US$57 million in cash and the closure of more than 3,700 illegal gambling dens which handled almost US$8 billion worth of bets. Specifically, during the 2018 FIFA World Cup, over 14,000 locations were raided worldwide, 19,000 people were arrested and US$142 million were recovered. Credit card and personal financial information are used to purchase goods in the name of marks or obtain unauthorized funds from the marks’ accounts. The data stolen may be stolen in one country and used elsewhere making it harder to trace. Stolen cards are valuable but the compromised card data is more valuable and is easier to trade on darknet markets. The data is then used to create fake cards or used for CNP transactions. Card skimming at ATMs or payment kiosks or phishing are common ways to obtain credit card information. Money laundering is concealing or disguising the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. It is frequently a component of other, much more serious, crimes such as drug trafficking, robbery or extortion. The investigation of money laundering usually goes along with the original fraud investigation. Financial fraud investigations seek to find the origins, patterns, flows, and locations of illicit income and reveal the networks involved. Law enforcement can then freeze or confiscate the illegally acquired assets, arrest the fraudsters, and prepare to prosecute them.

The author and psychologist Maria Konnikova said, “The best confidence games remain below the radar. They are never prosecuted because they are never detected … It’s not uncommon, in fact, for the same person to fall for the exact same con multiple times” (Konnikova, 2016: 16). Based on the exploration of human psychology offered in this chapter, it should be no surprise why it is hard to detect cons and why the same person would fall for the same con again and again. While there may still be a sucker born every minute, by understanding how cons work and their universal structure – the hook, the line, the sinker, and the blow-off/cool out – whether at work, as work, or after work, it will be easier to detect even the better cons and stop them before they take their next mark.
NOTES

4. To round out the top risks of death, lightning is 1:576,000; dog attack is 1:112,400; hornets, wasps, or bees is 1:63,225; gunshot is 1:6,905; and tripping or falling is 1:127. Source: US National Safety Council.
7. Because Western countries read from left to right, it is thought that the first digit of the price resonates with us the most and shoppers are more likely to buy something for $4.99 than $5.00.
8. “Sock puppet “originally referred to a false identity created by someone to speak to or about themselves while pretending to be someone else.

REFERENCES


