Prologue

Navigating the Shadows: The Erosion of Trust

As the world navigates post-pandemic uncertainties, elections are in full swing across the globe. Can we trust those elections to be honest? Hey, can we even trust that the cat video we just saw wasn't manipulated?

I'll open this updated version of *Manipulated* with a dialog with somebody who has been on the frontlines of spotting manipulation in a variety of settings for many years. He's someone who can shed some light on how today's technology is being used to design deceptions and, more importantly, how you can spot those deceptions to stop the bad guys from manipulating your all-important vote. Grab a cup of your favorite beverage and get ready for this chat with Frank Abagnale, whose incredible life story inspired the movie *Catch Me If You Can*.

INTERVIEW WITH FRANK ABAGNALE: MASTER OF DECEPTION MEETS THE AGE OF AI

Theresa: Frank, it's been great to know you through our mutual friends, including several at the FBI. Today, we'll be delving into a topic that's more relevant than ever: the intersection of technology with fraud and deception.

Let's kick things off by filling folks in on how you became a very young man on the run.

Frank: Certainly. I grew up in a town named Bronxville in New York. I attended a private Catholic high school in New Rochelle, New York.

At 16 in the 10th grade there was a turning point not only in my education but also in my family.

I vividly recollect the day when the school's Father entered my classroom and in- formed me that a Brother would accompany me to Family Court.

There, before a judge, stood my parents.

Their divorce hearing was in progress, and the judge sought my allegiance to one parent or the other. Overwhelmed, I turned and fled the court room. I wouldn't see my mother again until I was in my twenties. By the time my father left this world, I languished in a French prison.

As I learned to survive on my own, I was fascinated by the power of charm and quick thinking to get me out of tight spots. It started with small untruths and gradually es- calated to forging checks, assuming false identities, and pulling off elaborate cons. My ability to adapt and think on my feet became my greatest asset.

Theresa: With your expertise, you've transformed your life and now help organiza- tions prevent fraud. What techniques do you use to help organizations outsmart these tricksters?

Frank: After my stint as a con artist, I realized I could put my unique insights to good use. I've been working with various government agencies, corporations, and law enforce- ment to educate them about the ever-evolving tactics of fraudsters. My goal is to help them stay one step ahead by understanding the mindset and methodologies of criminals. It's all about knowing the enemy. I spill the beans on scammers' tactics so these organiza- tions can advance their knowledge and stay a step ahead.

Theresa: How do you think fraud has evolved in recent years?

Frank: You know, the landscape's shifted quite a bit since the days when a dapper con man could work his magic. Back then, being a "con man" was about that confidence, that charm that made people dance to your tune. Picture it: a polished appearance, a honeyed voice, and the ability to convince folks to do things they wouldn't dream of doing on a regular day: The classic art of persuasion.

But today? Well, that's a whole different tale. The digital realm has blurred those lines, making sure you never lay eyes on your mark, and they never catch a glimpse of you. See, that's the game-changer—this virtual dance, where you're just a voice on the line or a few lines in an email. The catch? You're chatting with someone who's kicking back in their Russian lair, pajamas on, coffee in hand. There's no emotion there, just a clinical pursuit of gain.

Back in my day, even the craftiest of crooks had a tad of sentiment. Even a bad apple would think twice before cleaning out their prey. Why? Because there was a connection, some sort of recognition that they had a face. A smidgen of conscience might say, "Let's not leave them completely desolate, shall we?" But in this digital masquerade, there's none of that. You're a cipher on the line, a stranger in the void.

So, as the wheels turn and time marches on, we find ourselves in a realm where de- ception thrives like never before. The numbers? Well, they've multiplied beyond belief. Why? Because it's a breeze to cast that net wide these days. Back when I used to school the folks at the FBI, the Nigerian scam was a thing, delivered via letters. A skeptic might ask, "Who's footing the bill for all those stamps?" Little did they know, those stamps were nothing more than forged tokens.

Now, skip to the present—a digital world where a single click sends ripples across the globe. I can fire off a torrent of 10 million emails, with just a tiny fraction—the same one-tenth of 1 percent—likely to bite. Technology's woven its magic, turning the globe

into a stage for the most intricate of scams. The boundaries have fallen, and we find ourselves facing devils from every quarter.

But here's the kicker. Even if I know where you're holed up, the game's not so simple. The world's become a small place, yet borders remain unyielding. The guy in Moscow might be on my radar, but it's a whole different ball game trying to nab him. You see, the authorities there are not exactly lining up to lend a hand. That chap in Moscow? He's feeling pretty darn safe, I can tell you that much.

Welcome to the new age of deception, where the battlefield's gone virtual, and the rules are being rewritten as we speak. In this digital arena, it's every bit as ruthless as it sounds—a shadowy dance that spans continents is made up of con men who hide behind the cloak of anonymity dressed in a coat of ones and zeros.

Theresa: How do you see the rise of AI and deepfakes affecting the landscape of fraud and manipulation?

Frank: AI and deepfakes have opened a Pandora's box of new opportunities for fraud- sters. With AI, fraudsters have a buffet of data to use to cook up convincing scams. Scammers can analyze massive amounts of data to create more convincing imperson- ations, making it easier to craft fraudulent documents and manipulate people's percep- tions. Deepfakes, on the other hand, allow for realistic audio and video manipulation, making it increasingly difficult to discern what's real and what's fabricated.

Theresa: Looking ahead, how do you envision the future? How do we fight back with- out spiraling into an Orwellian future? What steps can we take to avoid falling victim to this new wave of deception?

Frank: The future is both promising and perilous. As AI continues to advance, so will the capabilities of fraudsters. However, awareness is our best defense. Education is vital—teaching individuals to assess information critically, recognize signs of manipula- tion, and verify the authenticity of sources. Technology can also be harnessed to counter these threats, for example by using AI-driven tools that detect deepfakes and enhance cybersecurity.

Don't believe everything you see—question, doubt, investigate. Remember the tale of the boy who cried wolf? We need to be the villagers who fact-check. Secondly, we need the tech world's superheroes to create AI tools that identify and tag deepfakes. And lastly, we should teach our digital natives to wield their smartphones responsibly, not just for selfies.

Theresa: Can you provide an example of how AI and deepfakes could be combined to orchestrate a sophisticated fraud or manipulation campaign?

Frank: Imagine a scenario where a fraudster gains access to personal information about a high-ranking executive at a company. With AI, they can analyze the executive's com- munication patterns, style, and even their voice from public recordings. Then, using deepfake technology, they could create a convincing video of the executive discussing a sensitive financial matter or approving a fraudulent transaction. This video could be sent to colleagues or subordinates, manipulating them into taking actions that benefit the fraudster.

Theresa: You mentioned the importance of education and awareness. Could you offer practical tips for individuals and organizations to better protect themselves against these evolving threats?

Frank: First, skepticism is your friend. Always question unexpected requests, even if they appear to come from trusted sources. Verify the authenticity of requests through multiple channels, such as a phone call or face-to-face conversation. Second, stay informed about the latest scams and techniques. Criminals are constantly adapting, and knowledge is your best defense. Lastly, leverage technology to your advantage. Use AI- based tools to detect potential fraud and implement multi-factor authentication to add an extra layer of security. And of course, read this book. I had to get that plug in!

Theresa: Today, platforms such as Facebook, TikTok, WhatsApp, Snapchat, X, and Ins- tagram have become powerful tools for communication. How do you see these platforms being exploited to spread misinformation and disinformation?

Frank: Social media platforms have provided a global stage for information sharing, which can be both a blessing and a curse. Malicious actors have realized that these plat- forms offer a convenient way to disseminate false information, exploit vulnerabilities in people's understanding, and manipulate public perception. They can craft compelling narratives that resonate with specific groups, regardless of the accuracy or legitimacy of the information.

Theresa: To your point that the speed and reach of social media can amplify misin- formation, can you provide an example of how misinformation campaigns could have real-world consequences?

Frank: Let's say a disinformation campaign spreads false information about a new health treatment that claims to cure a severe illness. People desperate for a solution might start sharing the information without verifying its authenticity. This could lead to individuals making health decisions based on false promises, causing harm to themselves, and pos- sibly undermining legitimate medical efforts. Misinformation can erode trust in experts, institutions, and even science itself.

Theresa: Trust is undoubtedly a valuable commodity in today's digital age. Why is the widespread dissemination of misinformation and disinformation such a critical problem for society?

Frank: The danger lies in the erosion of our shared reality. When people are exposed to false narratives, they can become polarized and divided, undermining the foundation of a well-informed society. Misinformation distorts public discourse and influences critical decisions, from voting to public health practices. It threatens democracy, public safety, and the very fabric of truth.

Theresa: Given the complex nature of this issue, what strategies do you think individu- als and platforms can adopt to counteract the spread of misinformation?

Frank: Education is essential, once again. Individuals need to develop critical thinking skills and become more discerning information consumers. Fact-checking and verifying sources before sharing information can go a long way. As for platforms, implementing

robust content moderation, flagging mechanisms for false information, and supporting credible sources can help curb the spread of misinformation. We must collectively prioritize accuracy and truthfulness in our digital interactions.

Theresa: Collaboration between individuals and platforms is crucial for addressing this challenge. Looking forward, how can society balance preserving free expression with preventing the harmful effects of misinformation?

Frank: It's a delicate balance indeed. Free expression is a cornerstone of democratic societies, but that freedom comes with responsibilities. Platforms can establish clear guidelines that prohibit the spreading of false information that poses significant risks. Encouraging healthy and respectful discussions while swiftly addressing instances of deliberate misinformation can help maintain a thriving digital space that respects both freedom of expression and the well-being of society.

Additionally, investing in fraud prevention and cyber education from an early age is vital. Teaching digital literacy, critical thinking, and ethical behavior can empower indi- viduals to navigate the digital landscape safely.

Theresa: Creating guidelines and education—essential pillars for a safer future.

Finally, Frank, how do you respond to your detractors who might question your transformation from a con artist to a crusader against fraud?

Frank: I welcome healthy skepticism; it keeps us all on our toes. My journey is a testament to the power of redemption and transformation. While my past may have been riddled with deception, it also gifted me with a unique perspective on the world of fraud. The lessons I learned during my escapades now serve as valuable tools in my work to thwart deception and help others avoid falling into its traps.

Critics are entitled to their doubts, but actions speak louder than words. My commitment to collaborating with law enforcement, educating organizations, and contributing to initiatives that empower young minds speaks volumes about my dedication to turn- ing over a new leaf. It's like discovering your past is a battleground where you gather the skills to progress in life after the war is over. So, to my detractors, I say: judge me by my actions, not just by parts of my history. I hope that when I'm gone, people will remember me not for what I did or didn't do when I was young but for what I've done with my life for the past 50 years.

Theresa, remember, the more we understand deception tactics, the better equipped we are to protect ourselves and our society. And just because the pixels say it doesn't make it gospel. Stay sharp, stay curious, and stay cautious.

Theresa: Frank, thank you for your time and dedication to shedding light on these pressing issues. Your insights remind us of the importance of staying informed and vigilant in the face of evolving challenges. We remain indebted to your unwavering commitment to our collective vigilance.

End of interview