PROBLEM? RELAX. YOU'VE GOT THIS!

My Face Is Advertising Something I Never Bought

How to Document Impersonation, Organize Reports and Communication with Others, and Limit the Damage Without Convincing Every Viewer Individually



Max Paradox

My Face Is Advertising Something I Never Bought

How to Document Impersonation, Organize Reports and Communication with Others, and Limit the Damage Without Convincing Every Viewer Individually

Max Paradox

PROBLEM? RELAX. YOU'VE GOT THIS!

ISBN: 9788384839386

ALL-IN Rafał Płonkowski



CONTENTS

INTRO 5

Chapter 1 - When Your Face Starts Making Promises Without You 10

Chapter 2 - Why People Believe an Advertisement You Never Approved 17

Chapter 3 - The First Twenty-Four Hours Are Not an Olympic Event 26

Chapter 4 - Miracle Takedowns, Internet Vigilantes, and Other Excellent Ways to Make Things Worse 34

Chapter 5 - One Stolen Face, Six Advertisements, and a Very Confused Filing System 43

Chapter 6 - The Helpful Stranger Who Needs Your Password 51

Chapter 7 - You Don't Have to Delete Your Entire Life to Protect Your Face 60

Chapter 8 - When Your Fake Endorsement Arrives at Work Before You Do 69

Chapter 9 - Capture the Evidence Before the Advertisement Changes Its Mind 79

Chapter 10 - Write a Report That Gives Someone Something to Do 87

Chapter 11 - Mission Control for a Crisis That Refuses to Stay in One Folder 96

Chapter 12 - Someone Trusted Your Face and Lost More Than Their Patience 104

Chapter 13 - One Statement, a Hundred Questions, and the Right to Stop Explaining Yourself 113

Chapter 14 - The Advertisement Is Gone, but the Search Engine Has Excellent Memory 122

Chapter 15 - When the Impostor Accuses You of Being the Impostor 132

Chapter 16 - No Perfect Evidence, No Unlimited Budget, and No Spare Life 141

Chapter 17 - The Advertisement Comes Back Wearing a Different Hat 151

Chapter 18 - Retire from Internet Patrol Without Leaving the Door Open 160

Chapter 19 - The Emergency Instructions You Hope Never to Open Again 169

Chapter 20 - Your Face, Your Rules, and the End of an Unwanted Contract 177

INTRO

The first sign that something is wrong is an email from a stranger demanding a refund. Apparently, you persuaded him to spend $249 on an investment program, promised remarkable returns, and personally guaranteed that the whole thing was legitimate. He wants his money back. You read the message twice, wondering whether someone has confused you with another person. Then you open the attached screenshot. There you are, smiling confidently beneath a headline announcing that you have discovered an extraordinary financial opportunity. Your photograph is genuine. Your enthusiasm is entirely fictional. You've never heard of the program, let alone recommended it. Nevertheless, according to the advertisement, you're apparently its most devoted customer, unofficial spokesperson, and possibly the reason its marketing department received a Christmas bonus.

Your first instinct is to explain the misunderstanding. You reply that you have nothing to do with the company and never authorized the advertisement. Unfortunately, the stranger has already seen what looks like convincing evidence of your involvement. He has your photograph, your name, and a promotional statement presented as your personal recommendation. From his perspective, your denial might sound suspiciously convenient. Meanwhile, another person forwards the same advertisement to a colleague, and someone else leaves a comment asking whether the promised results are genuine. Your imaginary commercial career is expanding, while your real career has suddenly acquired an unpaid customer complaints department.

What makes impersonation particularly unsettling is the way it turns ordinary trust against you. A photograph is no longer merely a photograph when someone attaches a fabricated endorsement to it. A familiar face can persuade people to lower their guard,

especially when the advertisement resembles the polished promotional material they encounter every day. The person seeing it may not know where the picture originated or whether you approved its use. They simply see somebody who appears willing to put their reputation behind a product. You know the endorsement is false, but that knowledge isn't automatically available to everyone else. The gap between those two realities is where confusion, reputational damage, and sometimes serious financial harm begin.

You might imagine that the obvious solution is to get the advertisement removed immediately. Sometimes that is indeed an urgent priority, particularly when people are being encouraged to surrender money or sensitive information. But removing a suspicious publication isn't always as straightforward as clicking a button marked "This Is Absolutely Not Me, Thank You Very Much." The material may be displayed through an advertising account you cannot identify, linked to a website outside the platform, or reproduced in several different places. A fraudulent profile might imitate your identity while another account distributes the same photograph. Worse, the advertisement could disappear before you've preserved enough information to explain what happened. The result is a peculiar administrative nightmare in which you're trying to prove the existence of something that is no longer visible.

The opposite temptation is just as troublesome: attempting to investigate everything personally. You search for your name, inspect unfamiliar accounts, open numerous browser tabs, and try to establish who created the advertisement. Every discovery seems to generate three new questions. Is the company real? Did somebody steal your photograph from a public website? Was a genuine account compromised? Could the image or video have been manipulated? Is the person contacting you actually a victim, or another scammer hoping to exploit your concern? Before long, you've become the lead investigator in a case involving your own

face, despite having no investigative training and considerably more pressing things to do with your afternoon.

This book starts from a more manageable proposition: you don't need to solve every mystery before you can take useful action. You need to distinguish what you know from what you suspect, recognize which risks require immediate attention, and preserve the information that could help you make sensible decisions. A screenshot may establish what appeared on a screen, but it doesn't necessarily identify the person responsible. A suspicious profile might demonstrate impersonation without proving that your genuine account was compromised. A formal complaint can document an incident without guaranteeing that the material will be removed. Understanding these distinctions allows you to work with evidence rather than assumptions, even when the situation is moving faster than you'd like.

You'll discover how to preserve advertisements, messages, web addresses, and relevant context without turning your computer into a museum dedicated to your least favorite photograph. You'll learn to organize reports so you can identify which publication each response concerns, what has actually been done, and what remains unresolved. More importantly, you'll understand why the quality of a report matters more than the number of exclamation marks in its subject line. The objective is not to become a lawyer, cybersecurity engineer, or professional online detective overnight. It is to make informed choices, communicate clearly, and recognize when a problem calls for help from someone with the appropriate expertise.

Communication deserves particular attention because impersonation doesn't affect only what people see. It affects what they believe about you. Friends may ask awkward questions, professional contacts may become concerned, and strangers may assume you've endorsed something dubious. Trying to convince every individual separately can quickly become a second

occupation, with terrible working hours and no salary. A carefully prepared clarification, shared through an authentic and recognizable channel, can often serve people better than dozens of improvised explanations. It won't make every skeptic believe you, and it shouldn't require revealing your private records to satisfy their curiosity. Its purpose is to provide reliable information to people who genuinely need it.

There are also mistakes worth avoiding. The urgency of the situation can make questionable services promising instant removal appear attractive. Someone posing as a platform representative may request identification documents or login credentials under the pretense of resolving your complaint. Well-meaning acquaintances may encourage mass reporting, aggressive public accusations, or sharing the fraudulent advertisement so widely that the warning effectively becomes free promotion. Not every proposed solution reduces the harm. Some create new privacy risks, invite unnecessary conflict, or consume time without bringing the incident any closer to resolution. Learning when not to act can be as valuable as knowing what to do next.

None of this means you should minimize the consequences. If people have lost money, accounts have been compromised, threats have been made, or serious legal questions arise, the circumstances may require prompt assistance from financial institutions, relevant authorities, technical specialists, or qualified legal professionals. The available procedures and protections vary by service, jurisdiction, and the nature of the incident. No general guide can promise that every fraudulent publication will disappear or that every loss can be recovered. What it can offer is a practical way to evaluate the situation, reduce avoidable mistakes, and seek the right kind of assistance without pretending that a single clever trick can fix the entire internet.

There is one final cost that rarely appears in formal complaint forms: the energy required to live with the uncertainty. Even after a

publication disappears, you may find yourself searching for new copies, questioning every unfamiliar message, or hesitating to share an ordinary photograph. Protecting your identity matters, but protection shouldn't demand permanent surveillance of your own existence. A sensible response includes knowing when to check, when to escalate, and when to return your attention to the rest of your life.

Someone else may have decided that your face would make an excellent sales pitch. That decision doesn't give them ownership of your reputation, your time, or your future choices. You cannot dictate everything strangers publish or believe, but you can establish facts, protect important information, communicate through credible channels, and respond to genuine risks without chasing every rumor. Your face may have been recruited into an advertising campaign without your permission. The rest of you doesn't have to accept the job.

Chapter 1 - When Your Face Starts Making Promises Without You

Imagine discovering that you are the enthusiastic spokesperson for a company you have never heard of. Not through an employment contract, a flattering invitation, or even a suspiciously generous offer of free merchandise. You find out because somebody sends you an advertisement featuring your photograph beside the words, "I personally recommend this service." The company apparently specializes in helping people build successful online businesses. According to the promotional copy, you've achieved remarkable results, developed an entirely new lifestyle, and would happily encourage everyone to follow your example. This is impressive, considering that your actual experience with the company consists of staring at its advertisement and wondering who gave your photograph a second career.

The immediate temptation is to call the entire thing identity theft, fraud, or an elaborate conspiracy involving everyone whose name appears on the website. The anger is understandable. Somebody is presenting an invented version of your life as commercial evidence, and the possible consequences extend beyond an embarrassing photograph. People might believe you endorsed the service, trust its claims because of your apparent involvement, or question your judgment when the offer turns out to be questionable. Yet before deciding what to call the incident, it helps to understand precisely what has happened. Different kinds of impersonation create different risks, and the most effective response depends on recognizing those differences rather than choosing whichever accusation sounds most dramatic.

The first useful distinction concerns the difference between using your appearance and pretending to be you. Somebody might take a publicly accessible photograph and place it beside a

fabricated testimonial. That is one kind of problem. Creating an account under your name, answering questions as though they were you, and accepting payments from people who believe they are dealing with you introduces another. Gaining unauthorized access to your genuine account is different again. All three can involve the same recognizable face, but they don't necessarily involve the same method, level of access, or immediate danger. A stolen photograph does not prove a stolen password, and an imitation profile does not automatically mean that your legitimate account has been compromised.

Consider an ordinary professional headshot. You might have supplied it to an event organizer who published a speaker announcement, or displayed it on a professional networking profile. Somebody copies it and creates an advertisement claiming that you have personally benefited from a new business service. The picture may be entirely genuine, while the recommendation is invented. In another scenario, a stranger creates an account using your name and begins corresponding with potential customers. In a third, somebody edits an authentic interview to make an unrelated sentence appear to endorse a product. The visible result may seem similar to an unsuspecting viewer, but what needs investigating is not identical. Understanding this prevents you from approaching every suspicious advertisement as though it were evidence of a complete takeover of your digital life.

The difference between a photograph and a false identity

The most revealing question is often not whether your photograph appears in the material, but what the material suggests about your participation. An image used in a news report may identify you as somebody involved in a particular event. An advertising photograph accompanied by a first-person testimonial suggests something much more specific: that you experienced the product, formed an opinion, and agreed to share that opinion publicly. If none of those things happened, the advertisement is

manufacturing credibility through your identity. The distinction matters because the harm comes partly from the meaning attached to the image, not merely from the pixels that make up your face.

Suppose the advertisement reads, "After six months with this program, I finally achieved financial freedom," beneath your photograph and full name. You don't need to prove that the advertiser intended a particular criminal outcome to establish the basic discrepancy. You can truthfully say that you never participated in the program, never made the statement, and never authorized that endorsement. Those are concrete facts about your own actions. Whether the publication also constitutes a particular legal violation depends on circumstances and applicable law, which may require professional assessment. Keeping these questions separate allows you to describe what you know without pretending to possess information you haven't obtained.

The same care is needed when the advertisement appears to include your voice. An unfamiliar video showing you delivering a persuasive sales pitch might be digitally generated, assembled from authentic recordings, dubbed, or edited out of context. You cannot necessarily identify the technique by watching it once. Nor should you feel obliged to become a forensic video analyst before reporting that you never delivered the claimed endorsement. What you can establish personally is the difference between your actual involvement and the involvement attributed to you. Technical analysis may become important later, but a confident guess about how the material was created is not a substitute for evidence.

Names and photographs also behave differently across the internet. Two accounts can display identical portraits without being controlled by the same person. One website can reproduce promotional material prepared elsewhere without having created it. A company named in a misleading advertisement might itself be impersonated. These possibilities are frustrating because they complicate the attractive idea of finding one obvious villain with a

convenient contact address. Nevertheless, they are worth keeping in mind. The fact that a brand appears prominently in a suspicious promotion does not establish that the genuine business authorized it. Public accusations based on that assumption can create another dispute while leaving the original problem untouched.

There is a useful practical habit here: describe the observable conduct before attributing responsibility. "This account is displaying my photograph with a testimonial I did not provide" is a meaningful statement. "The owner of this company personally stole my identity and organized an international fraud operation" is a considerably larger claim. The second might make an excellent opening line for a television thriller, but it requires evidence that an advertisement alone cannot supply. By separating what is visible from what is suspected, you make your account more useful to moderators, advisers, and anyone else trying to understand the incident.

What is actually at risk?

Once you've established the basic nature of the impersonation, the next question is what the publication might cause people to do. A false endorsement of a harmless-looking product may still damage your reputation, but a fraudulent advertisement seeking bank details or account credentials presents additional concerns. A counterfeit professional profile that contacts your existing clients may disrupt business relationships. A fake message sent to relatives asking for emergency payments raises another kind of urgency altogether. Treating these cases as equally pressing makes it harder to recognize the situations in which delay could expose somebody to a serious and avoidable loss.

Imagine discovering a promotional website that uses your face to sell access to an exclusive professional community. It may merely display a fabricated testimonial, or it may invite visitors to submit payment information. Those details change the practical significance of the publication. If the advertisement creates a

credible risk that people will surrender money or sensitive information, prompt warnings and reports may be important. You do not have to complete the purchase process yourself to establish whether it is suspicious. Deliberately entering payment details or downloading unknown software in pursuit of proof could expose you to the very danger you are trying to prevent.

A different level of concern arises if messages are being sent from your genuine account without your knowledge. Unexpected login notifications, unfamiliar sessions, changes to recovery details, or outgoing messages you did not write are reasons to investigate account security promptly through official channels. That is not the same as discovering your photograph on an unrelated website. The latter may involve copying an image that was already publicly accessible. Confusing those situations can lead to the wrong priorities: spending hours composing a takedown request when an unauthorized person may still have access to your account, or unnecessarily resetting every password because somebody copied a profile picture.

Your personal circumstances also affect the consequences. A freelance consultant might be falsely portrayed as endorsing a competing service. A teacher might discover an advertisement implying participation in a questionable educational scheme. Someone whose work involves public trust could face awkward professional questions even when nobody loses money. It is not necessary to invent catastrophic possibilities to justify taking the incident seriously. The relevant question is what the particular publication could reasonably communicate to people who know you or rely on your judgment. That allows you to identify genuine concerns without automatically assuming that every stranger on the planet has formed an opinion about your commercial activities.

The scale of exposure is another source of uncertainty. Perhaps the person who alerted you saw a paid advertisement targeted to a particular audience. Perhaps the material circulated through

private messages. It might have been displayed widely, or it might have reached a relatively small group. One screenshot rarely establishes the answer. Even visible engagement figures may not reveal how many people noticed, believed, or acted on the endorsement. It is better to record the reach you can substantiate than to turn an unknown number into a terrifying estimate. Imagining that half the country has seen your imaginary testimonial may be emotionally compelling, but it doesn't make the estimate accurate.

Begin with a description you can stand behind

An effective first account of the incident can be surprisingly ordinary. Identify the material as specifically as you can, explain how it presents your involvement, and state what you know to be false. If you cannot determine the original publication date, say when you discovered it. If somebody forwarded the image without a source address, preserve that distinction. If the identity of the publisher is unknown, don't fill the gap with the name of the most convenient suspect. These simple choices create a description that can remain accurate even when later discoveries change your understanding of the situation.

For example, imagine writing: "On Tuesday afternoon, I received a screenshot of an advertisement showing my professional photograph and claiming that I recommend the service advertised. I have not used or endorsed that service and did not authorize this promotional use of my image. The original publication address has not yet been established." This doesn't tell the whole story, but it gives another person something concrete to work with. It also makes clear which details are known and which remain uncertain. Such a description can be expanded as new information arrives without turning every update into a correction of an earlier accusation.

You may discover that someone else has already shared your photograph in connection with an event, article, or professional

announcement. That does not automatically explain or justify its later use in a misleading commercial promotion. Permissions, lawful uses, and rights in photographs can differ according to context and jurisdiction. In particular, appearing in a photograph does not necessarily mean you own the copyright in it. A photographer or another rights holder may have separate rights. Understanding that distinction helps you avoid making the wrong kind of complaint while still recognizing that an invented endorsement can present a serious problem of its own.

At this stage, you don't need a complete theory about who planned the campaign or how sophisticated the technology was. You need an accurate picture of the conduct that is visible, the statements being attributed to you, and the risks that follow from those statements. That may feel less satisfying than immediately identifying a culprit, but it gives your decisions a sound foundation. A precise description can survive new discoveries. An elaborate accusation built on guesswork may collapse the moment one detail turns out to be wrong.

Somebody has taken a real element of your identity and attached a fictional commercial story to it. You cannot change that initial act, but you can refuse to let its confusion determine your next decisions. Start by understanding exactly what has been represented and what has not been established. Your face may be making promises on a stranger's website. That doesn't mean you have to start making promises of your own about facts you cannot yet prove.

Chapter 2 - Why People Believe an Advertisement You Never Approved

A colleague congratulates you on becoming the public face of a new online training company. You explain that you have never worked with the company and have no idea why your photograph appears in its advertising. Your colleague looks puzzled. "But it was a proper sponsored post," he says. "It even had comments from people thanking you." You realize that the advertisement has acquired something more powerful than a convincing design. It has acquired the appearance of legitimacy. The platform displayed it in the same format as countless ordinary promotions, several users appeared to accept it, and your recognizable face supplied the final detail. From your colleague's perspective, the whole thing looked sufficiently normal that questioning it never seemed necessary.

This is what makes false endorsements effective enough to be worth attempting. Their creators do not have to persuade an audience through a careful investigation of the evidence. They can rely on impressions formed during a brief encounter with promotional material. Most people do not approach an advertisement as though they are examining a suspicious financial statement. They notice a familiar person, a plausible claim, an attractive design, and perhaps a few encouraging comments. Then they continue scrolling. The advertisement may occupy only a moment of their attention, but the association between your identity and the product can remain. You have apparently endorsed something, and the audience may remember that impression long after forgetting where it originated.

It is tempting to call everyone who believes the advertisement gullible. That reaction provides a certain emotional satisfaction, especially when somebody insists that a professionally designed promotion must be authentic. Unfortunately, insulting the audience

does little to explain the problem or prevent further confusion. People regularly rely on familiar visual and social cues to navigate information efficiently. They cannot independently investigate every promotional statement they encounter. Those shortcuts are often practical, but they also create opportunities for deception. Understanding how the shortcuts work helps you communicate more effectively with people who have accepted a false claim without realizing it.

Credibility can be borrowed without permission

Imagine seeing a promotional photograph of somebody you know from a local business association. The person appears beside a statement praising a new service. You have previously found their professional advice useful, so the advertisement immediately feels more trustworthy than one featuring an unknown model. You may not consciously think, "I have verified this recommendation." Instead, recognition creates a favorable impression, and that impression influences how you interpret everything around it. The advertisement has borrowed credibility from an existing relationship without establishing that the person actually participated.

The strength of this effect depends on context. A photograph of a familiar professional may influence colleagues and clients differently from an image of an unknown person. A parent might pay special attention to a recommendation apparently made by another parent they know. A customer may be reassured by a recognizable local business owner. The impersonator does not need to create trust from nothing if some trust already exists between the audience and the person represented. They merely need to make it appear that this trust can safely be transferred to their offer. It is an extraordinarily convenient arrangement for the advertiser, who receives the benefit of somebody else's reputation without having to earn it.

This mechanism becomes particularly troublesome when the material combines real and fabricated details. Your name is correct. The photograph genuinely depicts you. The description of your profession may be accurate. Perhaps the advertisement even mentions a real event you attended or an authentic organization with which you are associated. These truthful details can make the invented endorsement seem like another piece of reliable information. An audience may accept the whole package without noticing where the verified facts end and the advertising fiction begins. The result is not necessarily a sophisticated forgery. Sometimes a genuine photograph and one carefully written false sentence are sufficient.

For that reason, it is useful to identify the exact point where the promotional message makes an unsupported leap. A legitimate photograph of you attending a professional conference does not establish that you recommend the software advertised beside it. A genuine quotation about the importance of education does not prove that you endorse a particular course. A real photograph of you holding a product does not necessarily mean you agreed to participate in a commercial campaign. When responding to an invented endorsement, you can explain the distinction rather than trying to discredit every element of the image. The photograph may be genuine. The commercial implication is the problem.

Even the layout of the advertisement contributes to the misunderstanding. A familiar button, recognizable platform interface, or ordinary sponsored-content label may make the material appear routine. But an advertisement being distributed through a platform is not proof that every statement within it has been independently verified. Advertising systems and moderation processes differ, and misleading material can sometimes appear despite rules intended to prevent abuse. Viewers may nevertheless confuse permission to display an advertisement with confirmation