SCAMS · CHAPTER 3

Case files

Scam patterns told as case files, from the first message to what it costs you. None of them is a real person or a real event, and each one ends with what to do.

FILE X3 CATEGORY SCAMS CHECKED 3 NOVEMBER 2026 READING 9 MIN
SECTIONS 9 EXHIBITS 3 STATUS OPEN

EVIDENCE ◆ Verified ◆ Reported ◆ Vivian's field notes

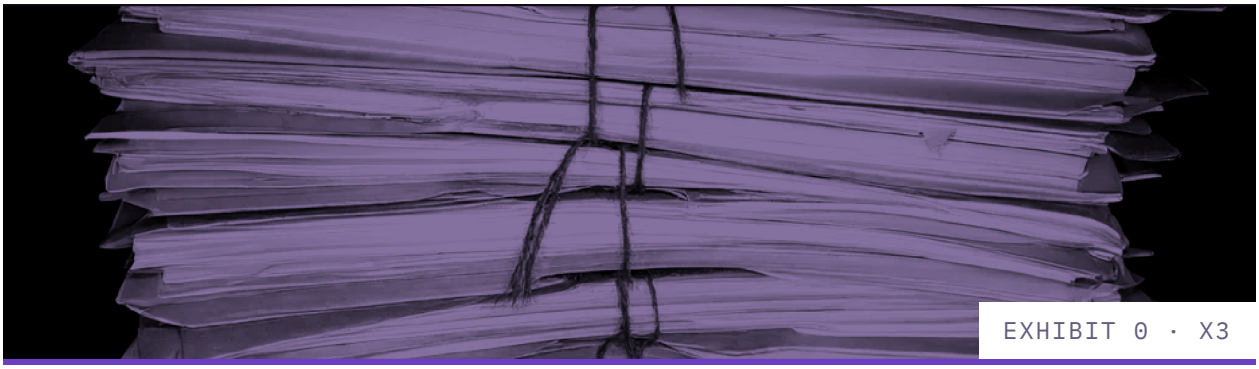


EXHIBIT 0 · X3

This chapter is not advice for your situation.

IN 30 SECONDS

01 A case file follows one scam from the first message to what it costs and how to get out.

02 No case here is a real person or a single real event. Each one is a pattern, rebuilt so nobody can be recognised.

03 Most of the harm comes through keys, payment routes and tools, more than from one villain.

04 A password, a login code or remote control of your device is never part of the game.

05 If you already sent, stop, keep the proof and tell someone you trust.

YOU WILL LEARN

- ✓ The six questions every case file answers.
- ✓ The verification fee, from the first message to the account vanishing.
- ✓ Why a promise never makes it safe to give someone a key to your accounts.
- ✓ Why a payment route that isn't yours can take a balance down with it.
- ✓ What to think about before you post a warning about anyone.

> *A case file is a story with the names taken out. I tell each one from the side of the person who gets the message, because that's the only place you can still refuse it. Read them once, calmly, and you'll recognise the real thing the day it shows up.*
>
> — VIVIAN

PART 01

How to read a case file

Every case file answers the same six questions: what it looks like, who it targets, why it works, what it costs, what to do, and where to report it. Use them on any offer, even one that isn't in this chapter.

No case here describes a real person or a single real event. Each one is a pattern, rebuilt from its parts. ◆ Press describes the scene as flooded with scammers who use stolen photos. ◆ The authors of a published study flag fraud, identity fraud included, as a risk that's still there. ◆ One victim quoted in the press said the emotional hurt outweighed the financial loss. ◆

PART 02

Case 1: the verification fee

How it starts. A new account writes to you first, with flattering words and a set of images that look expensive. In 2DFD the images may be stolen or generated art, so quality tells you nothing about who runs the account. ◆ Press reports fake accounts that reply to subs who post about findom and ask them to send a direct message. ◆

How it works (invented example)

1. **Contact**

   The account writes first and moves fast.

2. **The hook**

   “I only take serious subs.”

3. **The fee**

   “Pay a verification fee to prove you’re real.”

4. **The vanish**

   The account blocks you, or asks for a second fee.

Who it targets. New subs, and anyone who’s just posted that they want a dom. The scam is easy for anyone to start. ◆

Why it works. A fee to prove you’re real proves nothing, because nobody can check what it was for. It plays on wanting to be accepted and on the fear of missing your chance. ◆ Some real dommes also ask for payment first, to keep time-wasters away. ◆ The warning sign is a payment whose only purpose is to prove you’re serious, in a form that’s hard to reverse.

What it costs. The first fee, then a second ask under another name: insurance, an unlock fee, refund processing. Gift cards and crypto are hard to reverse once the funds are used. A card issuer, a bank or a gift-card company can sometimes block or reverse a payment that’s reported fast, so contact them right away. ◆

RED FLAGS

The tells

- Payment comes before any conversation, and it's called proof of something.
- The fee is asked in gift cards or crypto, instead of through a platform that keeps a record.
- There's a timer: now, or the offer is gone forever.
- Simple personal questions get no answer in the account's own words.

Counter. Send nothing before a real conversation. A real dom can wait an hour. The full list is in Spot a fake dom.

Where to report. On the platform where you met the account, with the messages and receipts attached. The longer way back is in If you already sent.

PROCEDURE

If you already sent

101	Stop sending, even to “unlock a refund”.
202	Keep the messages and the payment receipts.
303	Contact your bank, card issuer or the gift-card company right away, and ask whether the payment can be blocked.
404	Report the account on the platform where you met.
505	Tell someone you trust what happened.

PART 03

Case 2: the access request

How it starts. A dom asks for the login to a second social account, then for the code that arrives on your phone. Sometimes it’s a remote-desktop session. It’s framed as proof of loyalty or as the price of keeping the bond. ◆

Why it works. It comes at an emotional moment, wrapped in reassurance. A spoken promise protects nothing, and a login code lets someone else take over the account on the spot. ◆ Public guidance tells people not to hand control of a computer or phone to a stranger. ◆ A remote-access vendor says the same about anyone you don’t know or trust. ◆ In 2DFD nobody knows who’s behind the character, so in that sense every dom is a stranger. ◆

What it costs. The account, the private messages in it, and your name on whatever comes next. Shared logins take away the private space a sub needs to say no or to leave. ◆

TRY IT

Spot the flags (invented example)

Tap every message that shows a red flag. There are three.

Example conversation. Invented for this exercise.

THEM

Before this goes any further, I need proof that you're honest with me.

YOU

How can I show that?

THEM

Open a remote session so I can look. You can close it whenever you like.

Red flag 1. Remote control of your machine is a classic scam step, and being told you can close it protects nothing.

YOU

I'd rather not.

THEM

Then give me the code that arrives on your phone.

Red flag 2. A one-time code lets someone else take the account over on the spot.

At least the login of your other account.

Red flag 3. A login is a key to your identity. It proves nothing about honesty.

YOU

No. I don't share access, and I don't offer anything from my accounts.

VIVIAN'S FIELD NOTES

In my experience the request almost always comes at a weak moment: late at night, after a fight, after a slip. The timing is part of the method. A real dom never needs your password, and an honest question can be answered in words, so you owe nothing from your accounts.

◆

What to do. Refuse, offer nothing from your accounts, and state your own limit once. If the answer is more pressure, that's your answer. *Where to report.* On the platform where you met the account, and to the account's provider if you shared any code.

PART 04

Case 3: the tool that says one thing and does another

How it starts. A page promises a one-click helper. Everything stays local, nothing is charged unless you switch on a special mode, updates are automatic. A page is a promise. What the tool really does is in the code. ◆

Why it works. Most people read the page and skip the permissions. Chrome shows a permission warning at install. It also disables an extension after an update that adds a warning-level permission, until you accept it. ◆ Read the permission list first. Check a tool before you install it shows how, and Fake tools shows the patterns.

A worked example, the other way round. A first reading of a tool can suggest the worst, and a full reading can show a smaller risk. A tool whose updater can replace any file, sitting next to login tokens on the same computer, could take everything with one update. That's a different verdict from "malware". ◆

> VIVIAN'S FIELD NOTES
>
> *A false alarm costs trust as much as a missed one. Read the whole source, the updater and every network call included, before you use the word malware.*
>
> ◆

What it costs. Whatever the tool is allowed to reach: accounts and payments. ◆ *What to do.* Don't install anything you can't explain in one sentence. *Where to report.* To the store that distributes it.

PART 05

Case 4: the payment route that isn't yours

How it starts. A dom collects through a payment service. Some personas describe what they do falsely to a payment service, which breaks its terms and is why balances freeze. Or the platform that carries her wishlist loses its

payment partner and shuts down. Either way, the money sits on a route someone else owns. ◆

Why it matters to you. A payment service can close an account it finds was described falsely and hold the balance, and your payment goes with it. Terms differ from one service to the next, and they change. Anonymity ends where the money lands, because a payout is tied to a real identity. ◆

RED FLAGS

Signs that the route is shaky

- She asks you to describe your payment as something it isn't.
- She pushes you to pay outside the platform's visible route.
- She avoids plain words about money and about what a gift buys.
- She promises results a gift can't buy.

Counter. Say what the payment is, in plain words. If a dom asks you to call it something else, stop. The wrong label can freeze her money and yours.

What it costs. A frozen balance and a trail tied to a real identity. ◆ *Where to report.* To the platform, if a dom asks you to mislabel a payment. A dom who needs a legitimate route should read Getting paid.

PART 06

Case 5: three short patterns

REGISTER

Short patterns, from the side of the person on the receiving end

A

EXHIBIT

RED FLAG

A friendly dom messages you privately and asks for "a small thing" the dom you serve mustn't hear about

THE COUNTER

The secrecy is what makes it work. Keep one limit across everyone you pay, and tell the dom you serve. ◆

B

EXHIBIT

RED FLAG

Someone shows you a screenshot of a chat to make you doubt a dom

THE COUNTER

Anyone can edit the text of a web page and capture the result. Ask the dom directly, and don't leave over a screenshot alone. ◆

C

EXHIBIT

RED FLAG

A stranger steers you to a private messaging app with an offer of cheap or free video

THE COUNTER

Stay on the platform where you met, ignore it and report it. ◆

PART 07

Case 6: the click-to-post chain and the display account

How it starts. A chain of links drafts a post on your own account every time you click. The drafts escalate from a playful label to a confession to a payment announcement with a link. You're the one who publishes the text, under your own identity. ◆

A close cousin is the display account: a dom takes over a sub's public account and turns it into a showcase of his sends. Handing over a social account means losing control of your own identity, whatever the game calls it. ◆

PROCEDURE

Before you publish a draft that someone else wrote

101	Read the whole draft, all the way down.
202	Ask yourself whether you'd sign it with your own name a year from now.
303	Don't publish from an account tied to your real identity.
404	Decline the next link in the chain. Saying no costs nothing.

PART 08

Names, call-outs and proof

When you've been hurt, you may want to post a warning. A public warning can protect others, but weak evidence invites defamation claims, and the person

you name may have nothing to do with it. ◆ There's no foolproof way to screen out scammers. ◆

CLAIM 1

MYTH

"If I know the handle, I can say who's behind the persona."

FACT

Linking a handle to a real person without that person's own words is doxxing. It also invites payback, like mass reports from accounts the other side controls. ◆

TRY IT

A warning, or not

An account took a small amount from you and vanished. You have the messages. A friend is pushing you to post the account's name and its images on a public thread tonight.

A Post everything now

Not this one. The anger is fair, but the images may belong to a real person whose art or photos were stolen. You could name someone who had nothing to do with it. See Stolen art and persona theft.

B Report on the platform, keep the proof, and describe the pattern without the name

The right answer. This protects others and keeps your evidence intact. Share the pattern privately with people you trust.

C Say nothing and tell no one

Not this one. You carry it alone and the platform can't act. Tell at least one person you trust, and report it.

Six questions for any offer

Ask these every time

Can I trace the payment afterwards?

WHY IT MATTERS

A route that keeps a record for both sides protects both. Gift cards and crypto are hard to reverse once the funds are used.

Did money come before conversation?

WHY IT MATTERS

Some real doms do ask first. The warning sign is a payment called proof of something.

Is there a timer?

WHY IT MATTERS

A timer is there to stop you thinking. Wait an hour, then a day.

Does it need a key to my life?

WHY IT MATTERS

A password, a login code or remote access is never part of the game.

Would I sign this post with my own name?

WHY IT MATTERS

If not, don’t publish it from your own account.

Does the tool do only what its page says?

WHY IT MATTERS

Read the permissions before you install, and remove anything you can’t stop.

REMEMBER IT

- A case file is a pattern. Use its six questions on any offer.
- A fee to prove you're real proves nothing.
- A password, a login code or remote access is never part of the game.
- A payment route you don't own can vanish with the balance.
- Read a draft before you publish it, and report before you accuse.

SOURCES AND EVIDENCE

Check it

Every claim with its evidence level and its sources.

EVIDENCE LEVELS

Verified	Checked against the original source.
Reported	Stated by a serious secondary source read in full.
Community	Widely said in the scene; no document proves it.
Vivian's field notes	First-hand experience, not a study.
Unverified	Plausible, not proven yet.

01 Each one is a pattern, rebuilt from its parts.

◆

02 Press describes the scene as flooded with scammers who use stolen photos.

◆

Financial Domination Has a Scamming Problem (https://www.vice.com/en/article/financial-domination-has-a-scamming-problem)

Archive (https://web.archive.org/web/20260827104045/https://www.vice.com/en/article/financial-domination-has-a-scamming-problem/)

Accessed 3 November 2026

03 The authors of a published study flag fraud, identity fraud included, as a risk that's still there.

◆

Findommes, Cybermediated Sex Work, and Rinsing (McCracken and Brooks-Gordon, Sexuality Research and Social Policy 18(4), 837-854, DOI 10.1007/s13178-021-00609-3) (https://www.ebi.ac.uk/europepmc/webservices/rest/PMC8418458/fullTextXML)

Archive (https://web.archive.org/web/20261016030740/https://pmc.ncbi.nlm.nih.gov/articles/PMC8418458/)

Accessed 3 November 2026

04 One victim quoted in the press said the emotional hurt outweighed the financial loss.

◆

Financial Domination Has a Scamming Problem (https://www.vice.com/en/article/financial-domination-has-a-scamming-problem)

Archive (https://web.archive.org/web/20260827104045/https://www.vice.com/en/article/financial-domination-has-a-scamming-problem/)

Accessed 3 November 2026

05 In 2DFD the images may be stolen or generated art, so quality tells you nothing about who runs the account.

◆

06 Press reports fake accounts that reply to subs who post about findom and ask them to send a direct message.

◆

The Curse of the Fake Financial Dominatrix (https://melmagazine.com/en-us/story/the-curse-of-the-fake-financial-dominatrix)

Archive (https://web.archive.org/web/20260511185644/https://melmagazine.com/en-us/story/the-curse-of-the-fake-financial-dominatrix)

Accessed 3 November 2026

07 The scam is easy for anyone to start.

◆

Financial Domination Has a Scamming Problem (https://www.vice.com/en/article/financial-domination-has-a-scamming-problem)

Archive (https://web.archive.org/web/20260827104045/https://www.vice.com/en/article/financial-domination-has-a-scamming-problem/)

Accessed 3 November 2026

08 It plays on wanting to be accepted and on the fear of missing your chance.

◆

09 Some real dommes also ask for payment first, to keep time-wasters away.

◆

Financial Domination Has a Scamming Problem (https://www.vice.com/en/article/financial-domination-has-a-scamming-problem)

Archive (https://web.archive.org/web/20260827104045/https://www.vice.com/en/article/financial-domination-has-a-scamming-problem/)

Accessed 3 November 2026

10 The first fee, then a second ask under another name: insurance, an unlock fee, refund processing.

◆

11 Gift cards and crypto are hard to reverse once the funds are used.

◆

12 A card issuer, a bank or a gift-card company can sometimes block or reverse a payment that's reported fast, so contact them right away.

◆

13 It's framed as proof of loyalty or as the price of keeping the bond.

◆

14 It comes at an emotional moment, wrapped in reassurance.

◆

15 A spoken promise protects nothing, and a login code lets someone else take over the account on the spot.

◆

16 Public guidance tells people not to hand control of a computer or phone to a stranger.

◆

IC3 Issues Alert on Tech Support Fraud (https://www.cisa.gov/news-events/alerts/2018/03/29/ic3-issues-alert-tech-support-fraud)

Archive (https://web.archive.org/web/20250716102123/https://www.cisa.gov/news-events/alerts/2018/03/29/ic3-issues-alert-tech-support-fraud)

Accessed 3 November 2026

17 A remote-access vendor says the same about anyone you don't know or trust.

◆

TeamViewer and scamming (https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-and-scamming/)

Archive (https://web.archive.org/web/20260519191922/https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/security/teamviewer-and-scamming/)

Accessed 3 November 2026

18 In 2DFD nobody knows who's behind the character, so in that sense every dom is a stranger.

◆

19 The account, the private messages in it, and your name on whatever comes next.

◆

20 Shared logins take away the private space a sub needs to say no or to leave.

◆

21 In my experience the request almost always comes at a weak moment: late at night, after a fight, after a slip. The timing is part of the method. A real dom never needs your password, and an honest question can be answered in words, so you owe nothing from your accounts.

◆

22 Everything stays local, nothing is charged unless you switch on a special mode, updates are automatic.

◆

23 What the tool really does is in the code.

◆

24 It also disables an extension after an update that adds a warning-level permission, until you accept it.

◆

Permission warnings (Chrome for Developers, extensions documentation) (https://developer.chrome.com/docs/extensions/develop/concepts/permission-warnings)

Archive (https://web.archive.org/web/20261102194346/https://developer.chrome.com/docs/extensions/develop/concepts/permission-warnings)

Accessed 3 November 2026

25 A tool whose updater can replace any file, sitting next to login tokens on the same computer, could take everything with one update.

◆

26 That's a different verdict from "malware".

◆

27 A false alarm costs trust as much as a missed one. Read the whole source, the updater and every network call included, before you use the word malware.

◆

28 Whatever the tool is allowed to reach: accounts and payments.

◆

29 Either way, the money sits on a route someone else owns.

◆

30 A payment service can close an account it finds was described falsely and hold the balance, and your payment goes with it.

◆

31 Terms differ from one service to the next, and they change.

◆

32 Anonymity ends where the money lands, because a payout is tied to a real identity.

◆

33 A frozen balance and a trail tied to a real identity.

◆

34 Keep one limit across everyone you pay, and tell the dom you serve.

◆

35 Ask the dom directly, and don’t leave over a screenshot alone.

◆

36 Stay on the platform where you met, ignore it and report it.

◆

37 The drafts escalate from a playful label to a confession to a payment announcement with a link.

◆

38 You’re the one who publishes the text, under your own identity.

◆

39 A close cousin is the display account: a dom takes over a sub's public account and turns it into a showcase of his sends.

◆

40 Handing over a social account means losing control of your own identity, whatever the game calls it.

◆

41 A public warning can protect others, but weak evidence invites defamation claims, and the person you name may have nothing to do with it.

◆

42 There's no foolproof way to screen out scammers.

◆

The Curse of the Fake Financial Dominatrix (https://melmagazine.com/en-us/story/the-curse-of-the-fake-financial-dominatrix)

Archive (https://web.archive.org/web/20260511185644/https://melmagazine.com/en-us/story/the-curse-of-the-fake-financial-dominatrix)

Accessed 3 November 2026

43 It also invites payback, like mass reports from accounts the other side controls.

◆

Free, confidential helplines exist in most countries.

Find a helpline →