+44 204 591 6648



Research report for financial services firms in London, the South East and the East of England

The Financial Firm Fraud and Breach Report 2026

What 1,168 ICO breach reports, £41m of invoice fraud and the email records of 314 regulated firms say about the risks facing firms like yours.

November 2026

AT A GLANCE

Six numbers worth reading before your next board meeting

£41.3m



Lost to invoice and mandate fraud in the UK in 2025. 68% of it came out of business accounts.

44%



Of financial planning firms say between one and five of their clients were victims of cybercrime in the past year.

1,168



Data breaches reported to the ICO by finance, insurance and credit firms in the year to September 2026, up 16%.

38%



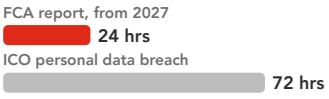
Of those reports reached the ICO more than 72 hours after the firm found the breach.

46%



Of the 314 regulated firms we checked have email that a criminal can fake in their name.

24 hours



From 18 March 2027, the FCA expects a report within 24 hours of a firm deciding an incident is serious enough.

How this report was put together

We went to the raw data rather than the usual round-ups. We cut the Information Commissioner's Office breach file down to the finance, insurance and credit sector, read UK Finance's 2026 fraud report and the FCA's new incident reporting rules in full, and checked the FCA Register record of every firm in our sample.

On 12 November 2026 we also read the public email settings of 314 regulated firms in London, the South East and the East of England. Every figure has its source in the margin beside it. Where a number is our own analysis, the margin says so.

SOURCES

Invoice fraud. UK Finance, Annual Fraud Report 2026 (2025 data), invoice and mandate scams.

44%. Saltus Financial Planning Growth Index 2026, by L.E.K. Consulting: 216 financial planning firms, survey concluded January 2026.

ICO reports. ICO data security incident trends, Q1 2019 to Q3 2026, sector "Finance, insurance and credit", one record per report. Analysis by AIS Technology.

Email settings. Public DNS records read by AIS Technology on 12 Nov 2026.

24 hours. FCA PS26/2, in force 18 March 2027.

INSIDE THIS REPORT

01 Your clients' money is the target 3

02 Breaches are rising again 6

03 Your name in someone else's inbox 9

04 The FCA's new rules 12

05 Nine things to do 14



PART ONE

Your clients' money is the target

The commonest way to steal from a financial firm's clients isn't to break into anything. It's to send one convincing email: new bank details, an urgent withdrawal, a change of account. We looked at what the latest figures say.

£41.3m
lost to invoice and mandate fraud in 2025

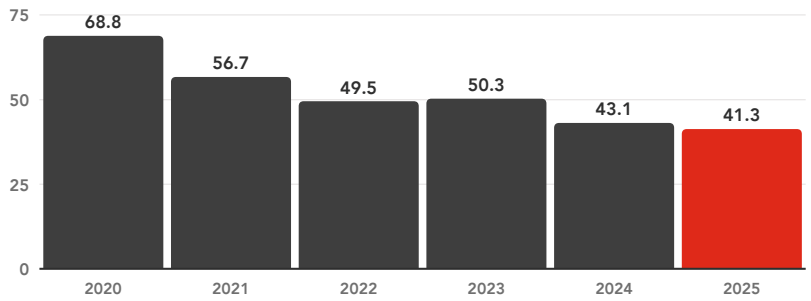
£28m
of it taken from business accounts

44%
of financial planning firms say clients were hit by cybercrime last year

Invoice fraud is falling. It still cost £41m.

UK Finance counts the losses from invoice and mandate fraud: the scam where a criminal intercepts an email, or takes over an email account, and tells the payer that the bank details have changed. Losses have fallen every year bar one since 2020, which is good news. They haven't gone away, and they land hardest on businesses.

Invoice and mandate fraud losses in the UK, £ millions



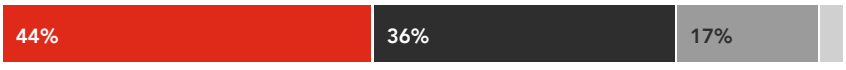
UK Finance, all victims. 2025 in red.

In 2025, £28m of the £41.3m was taken from business accounts, an average of about £23,000 for every business case. Businesses make large, regular payments, which UK Finance says makes a fraudulent one "harder to spot and stop".

And it reaches your clients

In the Saltus Financial Planning Growth Index, 44% of the 216 financial planning firms surveyed said between one and five of their clients had been victims of cybercrime in the past year. Only 36% said none had.

Financial planning firms: clients hit by cybercrime in the past year



One to five clients | **None** | **Unsure**

3% gave other answers

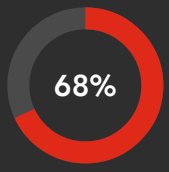
SOURCES

UK Finance. Annual Fraud Report 2026, "Invoice and mandate scam 2020 to 2025" table: total losses £68.8m, £56.7m, £49.5m, £50.3m, £43.1m, £41.3m. "68 per cent (£28 million) of invoice and mandate scam losses occurred on a non-personal or business account."

£23,000. Our arithmetic: £28.0m across 1,217 business cases in 2025.

Saltus. Financial Planning Growth Index 2026, L.E.K. Consulting. "44% say that between one and five clients have been victims of cybercrime, while 36% report no cases. 17% are unsure."

BUSINESS ACCOUNTS



of invoice and mandate losses in 2025 came out of business accounts: £28m.

How one email moves the money

UK Finance says this kind of fraud "often involves the criminal either intercepting emails or compromising an email account". Inside a financial firm, it tends to run in four steps.

01

Get into a mailbox

The firm's, or the client's. A phished password is enough when there is no multi-factor sign-in.

02

Watch

Read the thread quietly until a payment or withdrawal is due.

03

Change one detail

New bank details, a new address for a withdrawal, a "quick favour" before a deadline.

04

Move the money

The payment goes to an account the criminal controls and is passed on within hours.

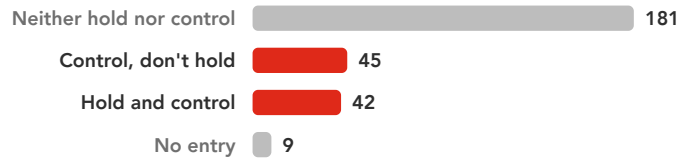
ILLUSTRATION · FICTIONAL FIRM

clientservices@marlowehirstwealth.co.uk	GENUINE
clientservices@marlowehirstwea1th.co.uk	LOOKALIKE
clientservices@marlowehirst-wealth.co.uk	LOOKALIKE

Where the client money sits

We read the FCA Register record of every directly authorised firm in our sample. A third of them hold or control client money, which makes a changed instruction more than an embarrassment.

Client money permissions, 277 directly authorised firms in our sample



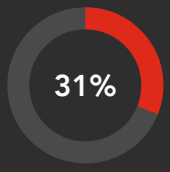
SOURCES

The four steps. Our description of the method UK Finance sets out in its Annual Fraud Report 2026: the criminal intercepts emails or compromises an email account, then claims the bank details have changed.

Domains. Invented to show the technique.

Client money. FCA Register API, firm records read by AIS Technology in November 2026. 87 of 277 firms hold or control client money; 9 had no entry.

CLIENT MONEY



of the directly authorised firms in our sample hold or control client money: 87 of 277.



PART TWO

Breaches are rising again

Every firm has to tell the Information Commissioner about a serious personal data breach within 72 hours. The ICO publishes every report it receives as open data. We took out the finance, insurance and credit sector.

1,168

breach reports in the 12 months to September 2026

247

were an email sent to the wrong person, the commonest breach of all

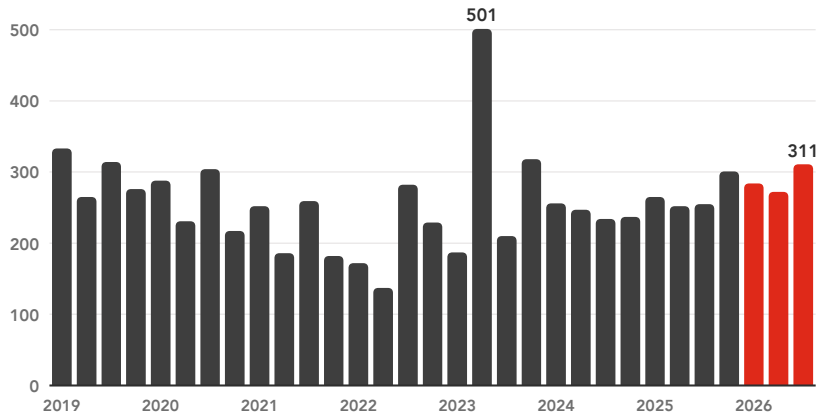
38%

reached the ICO more than 72 hours after the firm found out

Up 16% in a year, and still climbing

Finance, insurance and credit firms reported 1,168 breaches to the ICO in the 12 months to September 2026, against 1,009 the year before. The third quarter of 2026, with 311 reports, was the busiest since late 2023. The tall bar in 2023 is a one-off: a single quarter that the ICO's data shows at 501.

Breach reports from finance, insurance and credit firms to the ICO, by quarter



Q1 2019 to Q3 2026. 2026 quarters in red.

12 months to September	2025	2026	Change
All reports	1,009	1,168	+16%
Classed by the ICO as cyber incidents	366	398	+9%
Email sent to the wrong person	212	247	+17%
Phishing	163	207	+27%
Reported more than 72 hours after discovery	413	440	+7%

The commonest breach is an email sent to the wrong person. Phishing is close behind and rising faster. And 38% of reports were late: more than 72 hours after the firm found out, which is outside the deadline unless the delay can be explained.

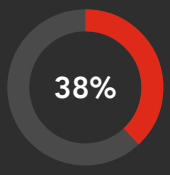
SOURCES

Source. ICO, Data security incident trends, open data file Q1 2019 to Q3 2026, published 26 Oct 2026. Sector "Finance, insurance and credit". One record per report reference, as the ICO advises. Analysis by AIS Technology.

What the data is. Breaches firms chose to report, so it shows what is reported, not everything that happens. The ICO notes its cyber and non-cyber categories are under review.

The 72-hour rule. UK GDPR Article 33.

LATE TO THE ICO



of finance breach reports arrived more than 72 hours after discovery: 440 of 1,168.

When the breach is at your supplier

The FCA says that "in 2025, over 40% of cyber incidents reported to us involved a third party". For a small firm that runs on outsourced IT, cloud software and a platform, that is most of the risk.

Capita

Fined £14m

ICO, October 2025 · Capita plc £8m and Capita Pension Solutions Limited £6m

22 March 2023
A malicious file is downloaded onto an employee's device.

Within 10 minutes
A high priority security alert is raised.

58 hours later
The device is finally quarantined. In that time the attacker gets into the wider network.

The result
6.6 million people's data stolen. Capita Pension Solutions handles pensions for more than 600 organisations, and 325 of them were affected.

✓ The alert worked. Nobody acted on it fast enough. That is a question to ask any IT provider: who reads the alerts, and how quickly?

Two lenses on the same risk

Financial advice firms reported just 34 material cyber incidents to the FCA across 2023 to 2025. In the same period the wider finance sector was sending the ICO about a thousand breach reports a year. The thresholds are different, so these aren't hidden incidents. They do show how much happens below the level the FCA counts, and the FCA's new rules, in part four, are designed to see more of it.

SOURCES

40%. FCA PS26/2, Operational incident and third party reporting, March 2026.

Capita. ICO, "Capita fined £14m for data breach affecting over 6m people", October 2025: an alert "within 10 minutes", but the device was not quarantined "for 58 hours".

34 incidents. FCA FOI2026/00094, February 2026: 9 in 2023, 13 in 2024, 12 in 2025, from firms in the advisers and intermediaries portfolio.

ALERT TO ACTION

58 hrs

between Capita's first security alert, raised within 10 minutes, and the device being quarantined.



PART THREE

Your name, in someone else's inbox

One email setting, called DMARC, tells Microsoft, Google and every other provider to reject messages that fake your firm's address. It costs nothing, and anyone can look it up. So we looked it up for 314 regulated firms.

314

FCA-regulated firms in London, the South East and the East checked on 12 November 2026

87%

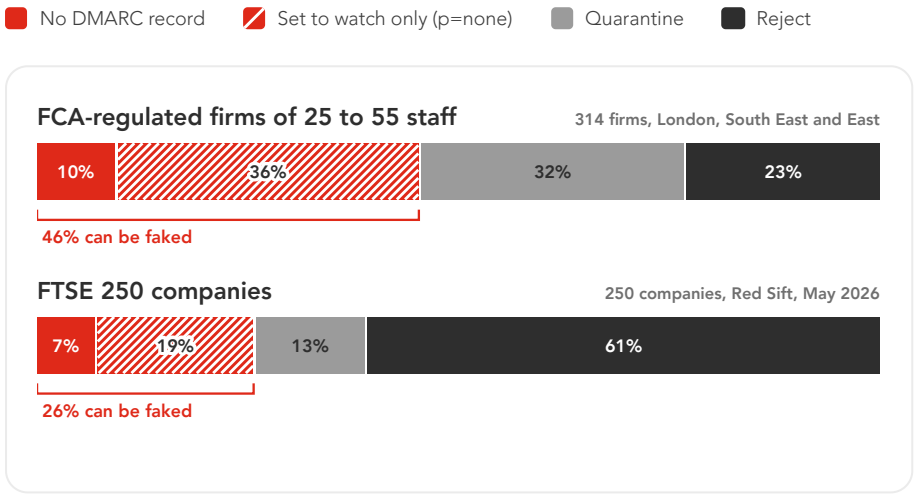
run their email on Microsoft 365

46%

have email that can be faked in their name

Almost half of firms like yours haven't switched it on

We looked at 314 FCA-regulated firms with 25 to 55 staff and no in-house IT team that we could find. 46% either have no DMARC record or have it set to "none", which watches and does nothing. Either way, an email can claim to come from the firm's own address and nothing tells the recipient's provider to stop it. For FTSE 250 companies the figure is 26%.



The firms that hold or control client money are no better protected than the rest: 46% of them can be faked, against 45% of firms that don't. Two more findings stood out.

52 of 113

firms on "watch only" haven't given an address for the reports. Nobody is watching.

48 of 127

firms paying for an email filter such as Mimecast can still be faked. A filter guards your inbox. DMARC guards your name in everyone else's.

SOURCES

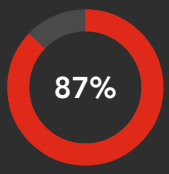
Method. Public DNS records read by AIS Technology on 12 Nov 2026. Each firm scored on the domain its staff send email from. No firm was contacted and no system was tested.

The 314 firms. FCA-regulated firms in London, the South East and the East of England with about 25 to 55 staff on LinkedIn and no in-house IT role we could find. 277 are directly authorised, including 6 payment firms.

FTSE 250. Red Sift, 12 May 2026.

Snapshot. Settings can change at any time. We publish totals only and never name a firm.

ONE PLATFORM



of the firms we checked run their email on Microsoft 365, where DMARC is a free setting.

What this setting won't do

DMARC stops one trick: email that claims to come from your exact address. It does nothing about a lookalike domain, a client's hacked mailbox, or a phone call from someone pretending to be your client. Those are behind much of the fraud in part one.

So treat it as the cheapest fix on the list rather than the whole answer. Each trick has its own defence.

The trick	What it looks like	What stops it
Your exact address, faked	An email that really does show @yourfirm.co.uk as the sender	**DMARC set to reject**
A lookalike domain	One character changed, a hyphen added, or .com for .co.uk	Clients who know you never change bank details by email, and domain monitoring
A hacked mailbox	A real account, yours or a client's, asking for a withdrawal or a change of details	Multi-factor sign-in, and a call to a number already on file before acting

CHECK YOUR OWN FIRM IN TWO MINUTES

01 Open any free DMARC lookup site. MXToolbox has one at `mxtoolbox.com/dmarc.aspx`.

02 Type your email domain: everything after the @ in your own address.

03 Find the value after `p=` in the result and read it against the list below.

p=reject	Fake email using your address is refused. This is where you want to be.
p=quarantine	Fake email goes to junk. Good, and one step from finished.
p=none	Watching only. Nothing is blocked.
Nothing found	No protection at all.

SOURCES

NCSC. Email security and anti-spoofing guidance, ncsc.gov.uk.

Moving to reject. Set up every service that sends email for you first (your CRM, your platform notifications, your marketing tool), read the reports for a few weeks, then tighten the policy.

THE NCSC'S ADVICE

"Having a DMARC policy of 'reject' on all of your domains is the best way to prevent spoofing of your email."

National Cyber Security Centre



PART FOUR

The FCA's new rules, in plain English

From 18 March 2027, every FCA-authorised firm has to report serious operational incidents, including cyber attacks and data loss, in a set format. For most small firms the report is short. Being ready to file it in time is the hard part.

18 Mar 2027
the date the rules come into force

10
questions on the short standard report most firms will file

24 hours
from deciding an incident is serious enough, at the most

What PS26/2 asks of a 40-person firm

WHO

Every firm with its own FCA permission. About 90% of firms, including almost all small ones, file a single short "standard" report. Payment firms report on a faster clock.

WHAT COUNTS

An incident that disrupts a service to people outside the firm, or affects their data. Near misses and planned outages don't count.

THE BAR

Serious incidents only: a risk of "intolerable levels of harm" to consumers, to the firm's soundness or to market integrity. A ransomware attack that exposes client data is the FCA's own example.

WHEN

As soon as practicable, and at the most within 24 hours of deciding an incident meets the bar. Payment service providers still report within 4 hours of detection.

What you will be asked

The standard report is short, but every field assumes you already know the answers. These are the things your IT provider has to be able to give you within hours.

- ✓ Whether the incident is open, resolved or closed
- ✓ Which threshold it triggered
- ✓ Disruption or data loss
- ✓ A description, with the likely root cause
- ✓ Your own severity rating
- ✓ The time it was detected
- ✓ What you plan to do to recover
- ✓ What you have already done
- ✓ When it was resolved

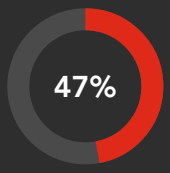
The ICO's 72-hour clock for personal data breaches runs alongside this one. A single incident can mean two reports, to two regulators, on two deadlines.

SOURCES

PS26/2. FCA, Operational incident and third party reporting, 18 March 2026. "c. 90% of the firm population" file "a single short form with 10 required questions". The report is expected "at the very most, within 24 hours of determining that it meets 1 or more of our thresholds."

Fields. FCA FG26/3, Operational Incident Reporting, Table 1.

NO PLAN YET



of finance and insurance firms have no formal incident response plan, in the government's 2026 survey.

THE FCA, ON OUTSOURCING

"While you may outsource the function, you can't outsource accountability for this function."

FCA guide for solo-regulated firms

WHAT TO DO

Nine things, in the order we'd do them

This week

- **Look up your DMARC setting.** Two minutes, using the steps in part three.
- **Check multi-factor sign-in covers every account.** Include admin, shared and service accounts, and anything set up years ago.
- **Name who decides if an incident is reportable.** The FCA's 24 hours runs from that decision, so someone has to own it.

This month

- **Write down the change-of-details rule.** Never act on new bank details or withdrawal instructions received by email without calling a number already on file. Tell every client, in writing.
- **Build a one-page incident log** with the fields the FCA will ask for: detection time, severity, root cause, actions taken.
- **Ask your IT provider three questions in writing:** who reads the security alerts, how fast they act, and how quickly they can give you what the report needs.

This quarter

- **Take DMARC from "none" to "reject".** Read the reports, fix the services that send email for you, then tighten the policy.
- **Run phishing training with a real test.** Phishing reports to the ICO from finance firms are up 27% in a year.
- **Rehearse one incident.** Take a plausible scenario and fill in the FCA's fields against the clock, before March 2027 makes it real.

SOURCES

A plan template. AIS Technology's free business continuity plan template includes a section on declaring an incident and the 72-hour rule: aistech.co.uk/guides.

Cyber Essentials. The government-backed scheme covers several of these controls, including multi-factor sign-in and removing unused accounts. ncsc.gov.uk/cyberessentials.

TALK IT THROUGH

020 4591 6648

If something in this report raised a question about your own firm, call AIS Technology. We're happy to talk it through.

info@ais.london · aistech.co.uk

SOURCES AND METHOD

Where every number comes from

ICO breach data. ico.org.uk/action-weve-taken/data-security-incident-trends, open data file Q1 2019 to Q3 2026, updated 26 Oct 2026. Sector "Finance, insurance and credit". One record per report reference. 12 months to September compares Q4 2024 to Q3 2025 with Q4 2025 to Q3 2026. Analysis by AIS Technology.

UK Finance. Annual Fraud Report 2026, covering 2025, invoice and mandate scam tables.

Saltus. Financial Planning Growth Index 2026, L.E.K. Consulting for Saltus, 216 financial planning firms, survey concluded January 2026.

FCA rules. PS26/2 Operational incident and third party reporting (18 March 2026); FG26/3 Operational Incident Reporting; SUP 15.18.

FCA incidents. FOI2026/00094, financial advice firms reporting cyber incidents, February 2026.

Capita. ICO, "Capita fined £14m for data breach affecting over 6m people", October 2025.

Government survey. DSIT Cyber Security Breaches Survey 2025/26, 30 April 2026, base 101 finance or insurance businesses.

FCA guide. "The Senior Managers and Certification Regime: Guide for FCA solo-regulated firms", July 2019, still the FCA's published guide.

FCA Register. Firm records read through the FCA Register API in November 2026.

Email settings. Public DNS lookups (DMARC, SPF, MX) through public resolvers on 12 Nov 2026, by AIS Technology. Results published as totals only. A setting shows what a firm has told other providers to do; it doesn't prove that a given fake email would arrive.

FTSE 250. Red Sift, "FTSE 250 DMARC report", 12 May 2026.

NCSC. Email security and anti-spoofing guidance, ncsc.gov.uk.

A note on the sample. The 314 firms are FCA-regulated firms in London, the South East and the East of England with roughly 25 to 55 staff on LinkedIn and no in-house IT role that we could find. They are not a random sample of all UK financial firms.

This report is general information and isn't legal or regulatory advice. Figures are correct as at 12 November 2026.

HOW THE NUMBERS WERE BUILT

89,591

Reports filtered

The ICO's full breach file, one record per report, cut down to the 1,168 finance, insurance and credit reports in the latest year.

277

Register records read

The FCA Register entry of every directly authorised firm in the sample, for status and client money permissions.

314

Domains checked

Public email settings for every firm in the sample, read on 12 November 2026.



ABOUT AIS TECHNOLOGY

IT support and cyber security for regulated firms

AIS Technology looks after the IT of financial services and professional firms across Essex, London and the South East: Microsoft 365, cyber security, a 24/7 help desk and on-site engineers. Our founder, Chris Dunham, worked in network security for the Home Office and for financial institutions before starting AIS.

We help our managed clients reach Cyber Essentials and Cyber Essentials Plus, and our optional compliance portal keeps the evidence an auditor, the FCA or a client will ask to see.

If anything in this report raised a question about your own firm, call us. We're happy to talk it through.

CALL

020 4591 6648

EMAIL

info@ais.london

WEB

aistech.co.uk

AIS TECHNOLOGY

The Financial Firm Fraud and Breach Report 2026. Published by AIS Technology, Wickford, Essex, November 2026. Contains public sector information licensed under the Open Government Licence v3.0. Images are illustrative. This report is general information and isn't legal or regulatory advice.