PayPoint

WHITE PAPER

Who You Pay Is the Risk

Beneficiary verification for supplier and payroll payments

A PayPoint case study in beneficiary risk and Confirmation of Payee

30,000+	1,300+	~20%	35m
UK store network	organisations served	of UK CoP requests	API calls / month

Executive summary

Almost all payment-security effort is aimed at the transaction: is the amount right, is it properly authorised, has it cleared through the right rail on the right day? This white paper argues that the largest and most persistent exposure sits somewhere quieter and far less examined — the **beneficiary**. The account you are paying is where value actually leaves the organisation, and it is the one variable every other control implicitly assumes to be correct.

Drawing on a structured review of PayPoint's own supplier and staff payments, this paper shows how systematically verifying who is being paid — using Confirmation of Payee (CoP) and related beneficiary checks — reduces fraud exposure, surfaces the silent decay of stored data, and saves operational time, without disrupting the business. Across more than £300,000 of supplier payments examined and dozens of payroll records reviewed, no money had gone to the wrong place — yet the act of checking still updated stale records, confirmed business-account status, corrected a widespread misunderstanding about what a routine 'checker' checks, and measurably lowered risk.

The core conclusion. The risk in a payment lives in the beneficiary details and how you manage them over time — not in the payment itself. Verify who you pay before the money moves, keep that verification current, and the single largest category of payment risk shrinks quietly, before it can ever cost you.

1. More than a terminal in the corner shop

Most people know PayPoint as the small terminal on the corner-shop counter — the place to top up a gas key, pay an electricity bill, or collect a parcel. With more than 30,000 stores across the UK, that retail network is genuinely vast: more locations than any bank or post office in the country. But the terminal on the counter is only a fraction of what the business has become.

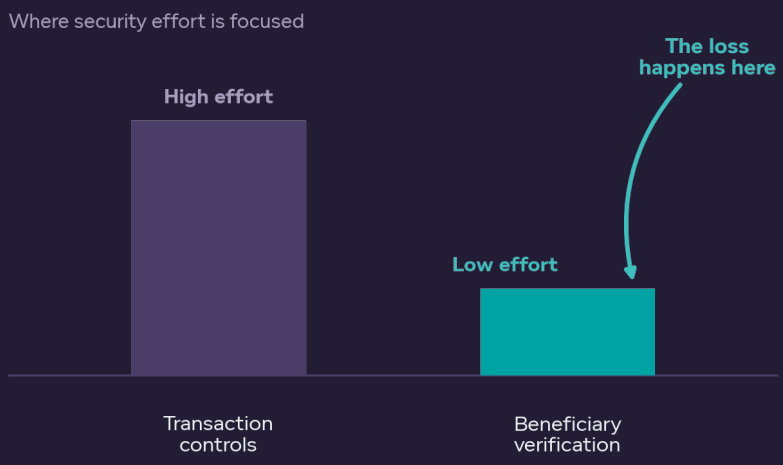
Behind that familiar front end, PayPoint is a financial-infrastructure company serving over 1,300 major organisations across government, utilities, housing, corporates and financial services. Through its MultiPay platform it processes payments worth billions across every channel — Direct Debit, Open Banking, card and cash. Alongside it sit Love2shop (employee rewards and prepaid cards), RSM2000 (a Bacs-approved bureau), and AperiData (real-time affordability assessments via Open Banking). And there is **obconnect**, a PayPoint subsidiary handling around 20% of all UK Confirmation of Payee requests — roughly 35 million API calls a month — which also delivered the national account-verification scheme for New Zealand.

30,000+	1,300+	~20%	35m
UK stores	organisations	of UK CoP	API calls / mo

That breadth is the premise of this exercise. PayPoint builds and sells the very tools that reduce payment risk to more than a thousand organisations. The obvious question is whether a business like that turns those tools on itself — which is exactly what the review described here set out to do.

2. The risk is who you pay, not how much

Payment security is habitually framed around the mechanics of the transaction: is the value correct, is it authorised, has it settled? These are necessary questions. But the dominant risk in a payment is not the sum or the mechanism — it is the beneficiary. If the account receiving the money belongs to the wrong party, every other control has already been satisfied; the payment simply leaves cleanly, correctly authorised, to the wrong place.



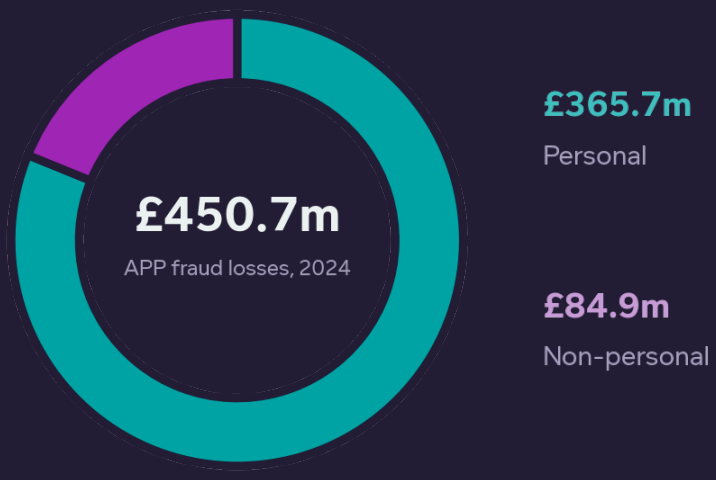
Security effort concentrates on the transaction — but the loss occurs at the beneficiary. (Illustrative)

2.1 · Why the beneficiary is the blind spot

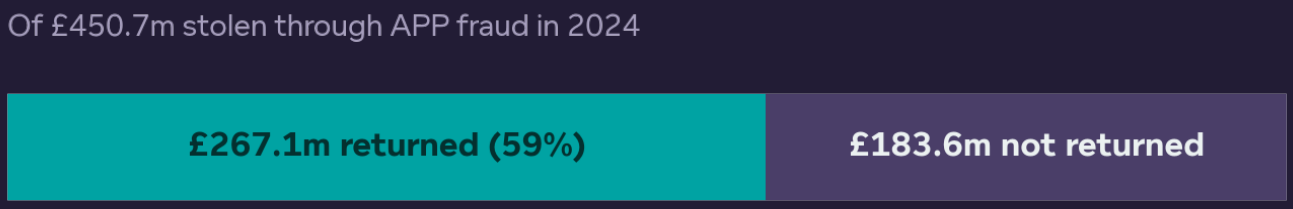
Beneficiary detail is uniquely exposed. It lives for a long time between checks; it changes for entirely legitimate reasons — companies re-bank, people marry, divorce and switch accounts; and that very legitimacy is what fraud exploits, because an attacker's whole objective is to make a malicious change look like one of the many innocent ones that happen every week. The result is a control gap hiding in plain sight.

2.2 · The national picture

The scale is well documented. Authorised push payment (APP) fraud — where a payer is deceived into sending money to an account they believe is legitimate — cost UK victims £450.7 million in 2024, according to UK Finance. The defining feature is that the payment itself is genuine and fully authorised; the deception is entirely in the beneficiary.



UK APP fraud losses, 2024, split personal vs non-personal. Source: UK Finance, Annual Fraud Report 2025.



Even with reimbursement, a large share of APP losses is never returned. Source: UK Finance, 2025.

2.3 · How it plays out inside organisations

For businesses, the same logic produces two well-worn attacks. The first is invoice redirection, often via business email compromise: a genuine invoice arrives but the bank details have been quietly altered, and the payment — correct in every other respect — lands in a fraudster's account. Because supplier payments are large and routine, this is the most valuable prize an attacker can take. The second is payroll diversion, where a salary is routed to the wrong account, whether through error, an un-notified bank change, or coercion.

2.4 · Why bank channels do not catch it

It is reasonable to assume the bank will catch this; in practice it usually cannot. Bank channels are historically a tool for viewing balances and moving money — not for attesting to who a beneficiary really is — and access is tightly limited, so the people onboarding a supplier or maintaining payroll rarely have the means to check within the banking interface at all. The capability to verify the payee has to be added deliberately, as a layer around the payment process.

3. The review — approach and method

A small team with deep transactional-banking backgrounds — clearing, agency, corporate and payment-provider work — was assembled to examine PayPoint's own payments with a fresh, constructively critical eye. This was never an exercise in finding fault; the internal teams were slick and notably open to challenge. The goal was to augment strong existing processes, not to grade them.

One pattern emerged quickly. PayPoint had robust controls for making payments, but drew on disparate information for onboarding the people and businesses it pays — the unavoidable consequence of integrating seven different companies without disrupting operations. Boiling the ocean is never a good plan; iteration is what lands. The team chose a single, high-value starting point: suppliers, where the values, and therefore the exposure, are greatest.

4. Suppliers — the highest-value target

Suppliers are the highest-risk beneficiary category because the values are larger, which makes supplier takeover the most valuable outcome a fraudulent actor can engineer. The review layered beneficiary verification on top of PayPoint's standard onboarding. Alongside the usual credit checks and company history, PayPoint used its own Confirmation of Payee service to confirm two things that matter enormously and are seldom checked together: that the bank account name matched the company being paid, and that the accounts being paid were **business accounts**, not personal ones.

The outcome speaks for itself. PayPoint has had no invoice fraud for three years — a period that coincides with the launch of its Confirmation of Payee service. As part of this review, more than £300,000 of supplier payments were examined to a deeper level of assurance. Every one matched; the changes that surfaced were organic drift, not wrongdoing. A clean bill of health — but one that only counts because it was verified rather than assumed.

5. Payroll — the harder, more sensitive problem

Staff payments are considerably harder to review. The data is highly sensitive, and — as expected — the review team could not see it directly; the approach PayPoint took to securing staff data was refreshingly strong. Salaries also carry a distinct and under-appreciated set of beneficiary risks.

The four principal beneficiary risks in staff payments, by relative severity.

#	Risk in staff payments	Why it matters and how it is mitigated
1	Error in the details the employee supplies	A transposed digit sends salary to a stranger; verifying name against account at onboarding catches it before the first run.
2	Employee moves bank and forgets to tell payroll	Salary is routed to a closed or reassigned account; periodic re-verification surfaces the change early.
3	Short-term temporary staff on- and off-boarded fast	High churn means details are rarely re-checked; a check at onboarding is the only realistic control point.
4	Modern-slavery or coerced salary diversion	Pay is directed to an account controlled by someone compromising the worker — beneficiary verification is one of the few controls that can expose it.

The first step was to empower the HR team to validate staff bank records, including a retrospective look at previous salary runs. The findings were revealing without being alarming: some staff used a hybrid of their name that differed from the account name; some were paid into a partner's or joint account; some used initials

where a full name was expected. Crucially, every member of staff was being paid to the right place — but the review still let PayPoint update married names, correct divorced names, and confirm the correct target accounts. In total, 63 staff records were updated for consistency: ordinary life changes, not wrongdoing.

> **A telling detail.** HR had a checker on their digital banking that validated the format of a payment file, and assumed it was a Confirmation of Payee check. It was not — it confirmed only that the file was in a Bacs-acceptable format. That gap led the team to a file-checking service that validates the format *and* confirms the records have been CoP-checked, turning a purely technical validation into a genuine beneficiary control.

6. What the findings tell us

- **Not all changes are malicious.** The overwhelming majority of beneficiary changes are innocent — which is exactly why they are dangerous to ignore.
- **Things change over time.** Businesses restructure and re-bank; people marry, divorce and switch accounts. Stored data decays continuously.
- **Fraud hides inside the innocent change.** Attackers use the ruse of a routine 'we've updated our details' to slip a malicious change past weak controls.
- **Suppliers are the highest-value target.** They are both the highest-risk point and the most valuable takeover, because the values are greater.
- **Bank channels will not do this for you.** The detection technology is not readily available in them, and access is historically restricted.

7. A practical framework

The lesson is not that PayPoint had a problem — it did not. It is that assurance comes from process rather than assumption, and that the beneficiary is where that process should concentrate. For any organisation making supplier or payroll payments, the review translates into a clear, implementable set of actions.

- **Verify who you pay before the point of payment.** Build the check into onboarding and ongoing maintenance, not the moment money moves.
- **Confirm the account is a business account, not personal.** A cheap check that removes a whole class of risk.
- **Correlate name changes with other records.** Turns a bare change into corroborated assurance and makes a fraudulent 'change' far harder to land.
- **Never rely on aged data.** Treat verification as recurring and event-triggered, not a one-off at onboarding.
- **Check at the file level, not just the format.** Ensure whatever validates your payment files confirms records have been CoP-checked.

£300k+	63	0	3 yrs
supplier payments verified	staff records updated	payments to a wrong account	no invoice fraud

8. Conclusion

PayPoint began this exercise confident that everything was correct, and in substance it was: no invoice fraud in three years, no salary paid to a wrong account, a clean bill of health across suppliers and staff. Yet the review still delivered tangible value — updated records, confirmed business accounts, a corrected assumption about what a routine 'checker' checked, lowered risk and time saved. Verification is not an accusation that something is wrong; it is the discipline that keeps 'right' true as the world changes around it.

The risk in a payment lives in the beneficiary details and how you manage them over time, not in the payment itself. Verify who you pay, keep that verification current, and correlate change against reliable sources, and the largest category of payment risk shrinks — quietly, continuously, and before it can ever cost you.

Source: UK Finance, Annual Fraud Report 2025 (APP fraud losses of £450.7m in 2024, of which £267.1m returned).