

How a Payment Lookup Oracle Confirms Predictable Identifiers

Badeesorn Sittikong

King Mongkut's University of Technology Thonburi

Tuul Triyason

`tuul.tri@sit.kmutt.ac.th`

King Mongkut's University of Technology Thonburi

Research Article

Keywords:

Posted Date: October 30th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10953971/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

How a Payment Lookup Oracle Confirms Predictable Identifiers

Badeesorn Sittikong · Tuul Triyason

Received: date / Accepted: date

Abstract Acquisti and Gross (PNAS 2009) demonstrated that structured national identifiers such as the U.S. Social Security Number are *predictable* from public data. A prediction, however, cannot be *confirmed*: the attacker never learns which guess is correct. We show that a national payment *resolution oracle* (the lookup that turns a phone number or national ID into an account holder’s name, deployed at population scale in Thailand’s PromptPay and in comparable systems across Asia and, since 2025, the EU) supplies exactly the missing confirmation step. We quantify (i) how the structure of the Thai national ID and mobile numbering plan shrinks the candidate space by a factor of 135 before any target-specific information; (ii) how a redacted identifier is reduced to a small candidate set (at most 10^k for k hidden digits) that a single oracle query per candidate disambiguates; (iii) how composition with an existing leak of 1 263 268 indexed national IDs converts prediction into deterministic, liveness-checked identity confirmation; and (iv) why the partial-name masking recently adopted by Singapore is weak on its own terms, leaving a given name unique for 51 % of a Thai corpus and a surname for 65.8 %, so it blunts human display-harvesting but not oracle-backed confirmation. A direct measurement across the apps of seven Thai banks finds the recipient name returned in full, unmasked,

in every case. All measurements are performed on the authors’ own accounts under an ethics protocol that forbids any enumeration of third-party identifiers. We conclude with concrete, quantified recommendations for scheme operators.

Keywords Proxy-addressed payments · PromptPay · Resolution oracle · Identifier predictability · De-anonymisation · Name masking · Verification of Payee · Instant payments · Privacy

1 Introduction

Proxy-addressed instant payment systems now serve billions of users. Instead of an account number, a payer enters a memorable proxy (a mobile number or a national ID) and, before authorising the transfer, is shown the recipient’s name so they can confirm they are paying the right person. This payer-facing name check is a genuine usability and anti-fraud feature: it prevents misdirected payments, and from October 2025 the European Union mandates an equivalent “Verification of Payee” for all eurozone providers [1]. Thailand’s PromptPay, in operation since 2017 and interlinked with neighbouring countries’ systems, is among the most mature deployments.

The same mechanism, however, answers a question it was never designed to answer. Its intended use is *confirmation*: the payer already knows who they intend to pay and checks the name. But the identical query also performs *discovery*: given only a proxy, anyone can obtain the associated person’s name, for free, without limit, and, crucially, without the subject ever learning they were looked up. We call this exposed function a *resolution oracle*: it maps an identifier to a real name, and it is open to the public.

B. Sittikong
School of Information Technology, King Mongkut’s University
of Technology Thonburi, Bangkok, Thailand
E-mail: badeesorn.sitt@kmutt.ac.th
ORCID: 0009-0004-2835-1539

T. Triyason (*corresponding author*)
School of Information Technology, King Mongkut’s University
of Technology Thonburi, Bangkok, Thailand
E-mail: tuul.tri@sit.kmutt.ac.th
ORCID: 0000-0002-5970-7751

This paper asks what that oracle is worth to an adversary, and it answers by connecting to a classic result. Acquisti and Gross [2] showed that structured national identifiers such as the U.S. Social Security Number are statistically *predictable* from public data. Their result stops at prediction: a predicted number cannot be confirmed, because no public function will tell the adversary whether a guess is right. A resolution oracle is exactly that missing function. Structure narrows the candidates; the oracle confirms the true one; and where the candidates are supplied by an existing data leak, prediction is bypassed altogether. Prediction becomes confirmation.

We make this concrete for Thailand, whose national ID and mobile numbering plan are highly structured and for which a large identifier leak already exists in public. We stress at the outset that the resolution feature is beneficial and that we do not advocate its removal; our target is the gap between what it was designed to do and what it also does, and the question of whether the mitigations now being adopted elsewhere actually close that gap.

Contributions.

- A threat model that names the payment *resolution oracle* as the confirmation primitive absent from SSN-era predictability work (§4).
- A quantification of Thai identifier structure: 43.2 bit naive space $\rightarrow$ 36.1 bit structured space ($\div 135$); mobile numbers $\approx$ 28 bits (§5).
- A partial-identifier de-anonymisation result: hiding k digits leaves $\leq 10^k$ (often $\leq 10^{k-1}$) candidates, oracle-confirmable (§6).
- A composition analysis with a real 1 263 268-record leak, delivering enrichment (name for name-less records, liveness, cross-source linkage) rather than mere re-identification (§7).
- An empirical collision analysis of partial-name masking over real Thai given-name and family-name corpora (the mask leaves a unique string for 51 % of given names and 65.8 % of surnames) and a direct measurement showing Thailand deploys *no* masking at all (§8, §9).

2 Background

PromptPay is Thailand’s national real-time retail payment scheme, operated over the National ITMX switch. Rather than a bank account number, a recipient registers a *proxy* identifier (a mobile number, a national ID or tax ID, an e-wallet ID, or a bank account number)

and *binds* it, through their bank, to one existing account. Registration is opt-in and per-account: a proxy is not created automatically, and a person with several accounts may bind different proxies to different accounts. A central directory, the ITMX Multi Proxy Platform, maps each proxy to its bound account so that any participating bank can route a payment addressed to that proxy.

Proxy types. The scheme admits several proxy types, and they differ sharply in how guessable they are, a distinction that matters for the attack (§5). A *mobile number* and a *national ID* are human-meaningful, externally recorded, and structured; a *tax ID* coincides with the national ID for a natural person; an *e-wallet ID* is an opaque 15-digit code; and a *bank account number* is bank-specific. Registration binds one such proxy to one account, and the same person may register different proxies against different accounts, so the returned name is a property of the *bound account*, not of the person globally (an observation we confirm in §9).

Addressing and the QR carrier. Payments are addressed either by entering a proxy directly or by scanning a QR code that carries it. The QR format is the Thai profile of the EMVCo merchant-presented specification [3], standardised by the Bank of Thailand [4]. In that profile the proxy is carried *in the clear* within the payload: a PromptPay credit-transfer template (tag 29) holds the mobile number, national/tax ID, or e-wallet ID as a plain substring, and a bill-payment template (tag 30) holds a biller ID derived from a tax or juristic-person number. Anyone who can read the QR image therefore already holds the proxy, before any lookup. In all of these flows (entering a number or scanning a code), the payer’s app resolves the proxy through the directory and displays the bound account’s registered name for confirmation before the transfer is authorised. It is this resolution-and-display step that we study as an oracle.

3 Related work

Identifier predictability. Acquisti and Gross [2] showed U.S. SSNs are statistically predictable from public birth data, prompting a policy debate on structured identifiers [5]. Subsequent work on other national schemes (e.g. analyses of leaked Chinese IDs, whose digits embed birth date and geography) confirms the pattern [6]. All of this work stops at prediction: it produces a posterior over candidates with no means of confirmation.

Re-identification from quasi-identifiers. A parallel literature shows that uniqueness in everyday attributes is the rule rather than the exception. Sweeney found that ZIP code, birth date, and sex identify roughly 87% of the U.S. population uniquely [7], motivating the k -anonymity model [8]; Narayanan and Shmatikov de-anonymised the Netflix Prize dataset by linkage to public film ratings [9]; and de Montjoye et al. showed that four timestamped points of credit-card metadata re-identify 90% of shoppers [10]. This body of work quantifies how little information isolates a person, but it too ends at a candidate or a probability. What distinguishes our setting is that the payment oracle supplies the confirmation these attacks lack, turning a likely match into a certified one at population scale and without the subject’s knowledge.

Payee verification. Confirmation of Payee / Verification of Payee, mandated for eurozone PSPs from October 2025 [1], is the same name-resolution mechanism viewed as a usability and anti-fraud feature. The privacy face of that mechanism (that it also resolves identities) has received little measurement.

Proxy-addressed payment systems. Security research on retail payment systems has concentrated on transaction integrity and application security rather than the identity-disclosure surface: Reaves et al. documented systemic cryptographic and authentication weaknesses across branchless-banking apps in the developing world [11], and Kumar et al. analysed UPI’s authentication flows and app implementations [12]. Both ask how an adversary moves money or hijacks a session; neither treats the payee-name resolution step as an information oracle, which is our subject. Singapore’s 2026 removal of PayNow nicknames is the closest policy touch-point: the operator’s stated *primary* purpose was to curb impersonation scams, and its materials describe the change as also adding “friction against name harvesting through PayNow’s lookup feature” [13], an acknowledgement of our concern, though as a secondary effect and without measurement. A subsequent commentary questioned whether alias removal in fact improves matters, arguing that lookup limits matter more than display format [14], to which the banks responded [15]. Our work differs from that exchange in kind: it is an empirical and analytic study of the disclosure itself rather than a policy argument about the nickname feature.

Leaks. Large-scale exposure of Thai national IDs through search-engine indexing has been documented [16]; we treat that corpus as a fixed input and study its composition with an oracle rather than the leak itself.

Gap. No prior work combines a *predictable* identifier with a *confirmation* oracle. That composition (prediction made certain) is our contribution. Table 1 places the major proxy-addressed systems on the two axes that matter for it: whether the resolution step discloses a name openly, and whether the addressable identifier is predictable from public data.

The EU design is instructive: Verification of Payee returns only a match/no-match against a payer-supplied name, disclosing far less, and is keyed on an IBAN that is not derived from public data. It sits at the safe corner of both axes; PromptPay sits at the dangerous one.

4 Threat model: the oracle as a confirmation primitive

4.1 Setting

Let $\mathcal{I}$ be the space of syntactically valid identifiers of a given type (national ID, mobile number). Let $\mathcal{A} \subseteq \mathcal{I}$ be the *assigned* identifiers (those bound to a real account holder), and let $\text{name} : \mathcal{A} \rightarrow \Sigma^*$ map an assigned identifier to its registered account-holder name. A *proxy-addressed payment system* exposes a *resolution oracle*

$$O(x) = \begin{cases} \text{name}(x) & x \in \mathcal{A} \\ \perp & x \notin \mathcal{A}, \end{cases}$$

so that a payer entering identifier x is shown the recipient’s name before authorising a transfer. The oracle is (i) *open*: any party with a payment app may query it; (ii) *unauthenticated* with respect to the subject: the holder of x is neither asked nor notified; and (iii) *practically unmetered* at the granularity of ordinary use. Property (ii) is what distinguishes an oracle query from an ordinary account lookup: the target cannot observe that a query occurred.

4.2 Baseline: prediction without confirmation

The predictability results of Acquisti and Gross [2] can be cast as an adversary who, from public auxiliary data z about a target, forms a posterior $\Pr[X = x \mid z]$ over candidate identifiers. Their central limitation is structural rather than statistical: even a sharp posterior yields no *certificate*. The adversary cannot tell a correct guess from an incorrect one, because the U.S. SSN exposes no oracle: there is no public function that, given a candidate SSN, returns a confirming signal. Prediction therefore terminates in a probability, not a fact.

Table 1 Proxy-addressed payment systems by name disclosure and identifier predictability. The attack of this paper needs both an open oracle and a predictable identifier.

System (country)	Name shown to payer	Addressable identifier
PromptPay (TH)	full, unmasked (§9)	national ID, mobile (predictable)
PayNow (SG)	partially masked since 2026 [13]	mobile, NRIC (predictable)
UPI (IN)	full (registered name) [12]	mobile/VPA (semi-predictable)
PIX (BR)	full (registered name)	CPF, mobile (predictable)
EU VoP (EU)	match/no-match by design [1]	IBAN (not guessable)

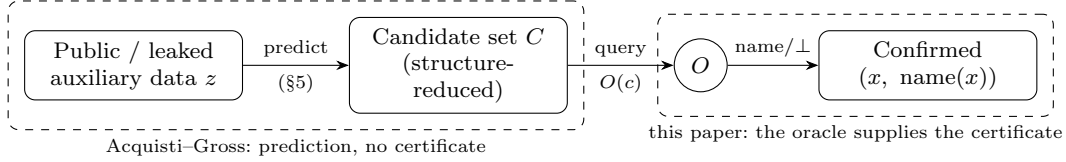


Fig. 1 Prediction becomes confirmation. Prior work reaches a candidate set but cannot verify a guess; the resolution oracle O supplies the missing certificate, and an existing leak can replace the prediction step entirely.

4.3 The confirmation step

An oracle O supplies precisely the missing certificate (Figure 1). Composition proceeds in three regimes of increasing adversary power, all of which we *analyse* but only the trivial self-referential case of which we ever *execute* (§9, Ethics):

Structure $\rightarrow$ confirmation. Section 5 shows the check digit and the geographic and person-type encoding shrink $\mathcal{I}$ to a structured subset $\div 135$ smaller, and reduce a *partially redacted* identifier to a candidate set C with $|C| \leq 10^k$ (§6). A single query $O(c)$ per candidate returns $\perp$ for all but the real one, collapsing C to a point.

Leak $\rightarrow$ enrichment. Given an existing corpus of assigned identifiers (§7, $|\cdot| = 1\,263\,268$), the search step vanishes entirely. Each record is one query from a confirmed name (where the leak lacks one), a liveness signal ($x \in \mathcal{A}$ today), or a cross-source linkage (two identifiers resolving to one name).

Masking as attempted mitigation. Where the operator returns a *masked* name $m = \mu(\text{name}(x))$ (§8), the adversary who holds a candidate name n needs only test $\mu(n) \stackrel{?}{=} m$. Masking degrades *discovery* of an unknown name but not *confirmation* of a hypothesised one, exactly the adversary that composition produces.

4.4 Adversary and scope

The adversary is any member of the public: no privileged access, no credentials, no malware; only a payment app, public auxiliary data, and, in the strongest regime, a leak that already exists in the wild. The target is a specific individual or a population thereof. The

adversary’s goal is not to move funds but to obtain, at scale and unobservably, a confirmed binding of identifier to identity (and, via liveness, to an active financial account).

We stress the boundary between *analysing* this adversary and *instantiating* it. Every quantitative claim in §5–§7 is arithmetic over public parameters and published datasets. The only live queries we run (§9) are $O(x)$ for identifiers x the authors themselves hold. We never query an identifier belonging to a third party, and we never enumerate. This is both an ethical commitment and, under the Thai Computer Crime Act B.E. 2550, the line separating authorised use of one’s own account from an offence.

5 The identifier space is small and structured

The Thai national ID is a 13-digit number whose thirteenth digit is a mod-11 check digit fully determined by the first twelve; digits 2–5 encode the province and district of registration and digit 1 the person type (one of eight categories).¹ These constraints turn a naive 10^{13} string space into a much smaller structured one (Table 2).²

¹ Layout per the Department of Provincial Administration [17]: digit 1 = person type (1–8); digits 2–3 = province; digits 4–5 = district; digits 6–12 = registration sequence; digit 13 = check digit. Constants in Table 2 are documented as labelled assumptions in `rq4.idspace.py`.

² The check digit is computed mod 11 and reduced to a single decimal digit; it is a deterministic function of the first twelve, so exactly one valid thirteenth digit exists per prefix and the “ $\div 10$ ” reduction in Table 2 is exact. In the partial-recovery setting (§6), where the check digit is instead *observed* and interior digits are hidden, the mod-11-to-decimal reduction makes the residual counts approximate rather than exact.

Table 2 Structured reduction of the Thai national-ID space. Entropy in bits, $\log_2$.

Space	Candidates	Entropy
Naive (any 13 digits)	1.0×10^{13}	43.19
Valid check digit (d_{13} fixed)	1.0×10^{12}	39.86
+ valid person-type & geo code	7.4×10^{10}	36.11
Actually assigned ($\sim$ populace)	1.0×10^8	26.58

Structure alone removes 7.1 bits ($\div 135$) before any target-specific information. We are candid that structure is the smaller lever: the population constraint in Table 2 removes a further 9.5 bits ($36.11 \rightarrow 26.58$), more than structure does, and once an existing leak supplies assigned identifiers directly (§7) neither reduction lies on the critical path. This does not weaken the argument so much as relocate it. Whatever narrows the field, whether identifier structure, the finite size of the populace, or a leak, the resolution oracle is what certifies the surviving candidate; the search-space arithmetic only sets how much work the oracle must do, not whether it succeeds. Crucially, the oracle then separates the $\sim 10^8$ assigned identifiers from the $\sim 7.4 \times 10^{10}$ valid-but-empty ones *for free*: a $\perp$ response is itself information. The Thai mobile plan is similarly constrained: numbers are 0 followed by a prefix in $\{6, 8, 9\}$ and eight digits, giving 3×10^8 (≈ 28 bits), against a naive 10^9 .

Which proxies are attackable. The attack requires an identifier that is both *predictable* (small structured space, or already leaked) and *something the adversary can plausibly hold about a target*. National IDs and mobile numbers qualify: they are structured, widely recorded, and frequently leaked. E-wallet proxies (e.g. TrueMoney, the government G-Wallet) are the exception. Although the oracle resolves them too, a wallet ID is an opaque ~ 15 -digit number carrying no public-data structure and is not something an adversary knows about a target in advance; it is neither predictable nor a natural starting point. The vulnerability is therefore specific to *human-meaningful* identifiers, which is itself a design signal: routing over opaque, non-guessable proxies is one structural mitigation (§8 discusses the display side).

6 Partial-identifier recovery

Redacted documents routinely reveal some identifier digits and hide others. Hiding k digits leaves at most 10^k candidates by direct counting; when the check digit is among the visible ones it further ties the hidden digits to the rest and removes a factor of ten (Table 3). A single oracle query per candidate then confirms the

Table 3 Candidates remaining when k digits of a national ID are hidden. Column 2 hides k arbitrary digits; column 3 is the case in which the check digit is *visible* and k interior digits are hidden, so the check equation ties the hidden digits to the visible ones and removes a further factor of ten; this is the situation in the worked example below and in typical redacted documents.

Hidden digits k	$\leq$ candidates	with the check digit visible
2	100	10
3	1,000	100
4	10,000	1,000

real one. This is the cleanest instance of the oracle-as-confirmation primitive: the adversary is not searching blindly but confirming a tiny hypothesised set, the operation the lookup was built to perform, turned against a target it was not built to serve. *We report the counts; we never run the lookups.*

7 Composition with an existing leak

A recent study documents 1 263 268 Thai national IDs already indexed by search engines [16]. Naive guessing hits a real ID roughly once per 10^5 tries; the leak removes the guessing step entirely. The oracle then *enriches* each leaked record rather than merely re-identifying it:

1. **Name-less records:** IDs appearing without an adjacent name gain one.
2. **Liveness:** a stale (id, name) pair is confirmed to be an active account today.
3. **Cross-source linkage:** an ID from one corpus and a phone from another that resolve to the same name are confirmed co-referent, merging partial profiles.

Two boundaries keep this claim honest. The oracle does *not* reveal the destination bank: the Thai transfer screen displays only the recipient’s name.³ And it does *not* “turn numbers into names” where the leak already carries names, so the contribution is enrichment of what the leak lacks, not wholesale re-identification.

How large is the name-less subset that the oracle can fill? The source study does not report it directly; it notes only that exposed records “typically” carried full names alongside the ID, and, by its authors’ own admission, does not quantify the proportion appearing without a name [16]. What it does report is a file-type and institutional breakdown. By format, 81.7% of the IDs came from spreadsheets, 19.1% from PDFs, and 0.3% from Word documents; spreadsheets are precisely the

³ Verified by direct observation across issuers; the ITMX Multi Proxy Platform resolves the bank internally without surfacing it.

format in which a column of IDs can appear detached from names (separate sheets, filtered exports, pivot outputs), so the name-less subset is plausibly non-trivial, though we make no numeric claim the source cannot support. By source, 756 278 of the IDs sit on `.go.th` government domains, 409 012 from Ministry of Interior agencies alone, and 133 396 from the Office of the Basic Education Commission, the last being *schoolchildren*, exposed through primary- and secondary-school registries together with their names, class, and address [16]. That a six-figure subset concerns minors sharpens the stakes: for these records a name is already present, so the oracle’s marginal contribution is liveness and linkage rather than naming, but it confirms that a live financial-account binding exists for an identifier belonging to a child.

Worked example (illustrative, fictitious). To make the composition concrete without any real data, consider a leaked spreadsheet row that lists a national ID but leaves the name column blank, with two of the thirteen digits illegible from a scan: say the row shows a valid-looking ID with digits at positions 9 and 12 unreadable. (1) *Structure.* The check digit at position 13 is determined by the other twelve, so once positions 9 and 12 are the only free digits, at most $10^2 = 100$ candidate IDs are consistent, and the check-digit constraint typically removes a further factor of ten. (2) *Confirmation.* Each candidate is one oracle query away from either a name or $\perp$; the blank name column is filled and all but the real candidate are eliminated. (3) *Enrichment.* If a second leaked file lists the same person’s mobile number, resolving it returns the same name, confirming the two records are co-referent and merging them. No step guesses blindly: structure supplies a handful of candidates and the oracle supplies the certificate. We present this only as an analysis; we ran no such queries (§4, Ethics).

Scale, as a bounded range. We resist a single headline figure and instead bound the affected population. The leaked corpus is 1 263 268 indexed IDs, about 1.9 % of the population. The oracle’s *name-completion* contribution applies to the name-less subset: at a deliberately low name-less fraction of 1 % to 10 % this is 13 000 to 126 000 records that gain a name they did not previously carry. The *liveness* and *linkage* contributions, by contrast, apply to records that already carry a name (up to the full 1 263 268), since each can be confirmed to be an active account today and cross-linked to other leaked identifiers resolving to the same person. The oracle thus converts a static leak into a live, name-complete, cross-linked dataset; the name-completion piece alone reaches

tens of thousands even under conservative assumptions (computation in `rq5_scale.py`). These are bounds, not measurements: we neither ran the lookups nor possess the name-less fraction the source did not report.

8 Does masking help? A collision analysis

From 6 June 2026, Singapore’s PayNow returns a partially masked name in place of a user-chosen nickname [13]. On ABS’s own published examples the mask preserves, for every word, its exact word count, its exact length, and, crucially, its first $\lceil L/2 \rceil$ characters, not merely its initial (Table 4): *Jacqueline* $\rightarrow$ *Jacqu-----* and *Jonathan* $\rightarrow$ *Jonat---* each expose five leading letters. Only the trailing half is hidden.

Revealing the first half of a name, rather than an initial, is decisive, and we quantify it directly on a public corpus of 8273 distinct Thai given names [18]. We compute on the names as PromptPay actually displays them, in *Thai script*, so the question we answer is concrete: were Thailand to adopt the ABS mask on Thai-script names, how many candidates would it leave?⁴ Two names are indistinguishable under the mask exactly when they share the same length and the same leading $\lceil L/2 \rceil$ characters; for each name we count how many others collide with it, which is the residual candidate set a payer holding the masked string faces (Table 5, computation in `rq2_masking.py`). The mask leaves a *unique* given name for 51 % of the corpus and at most two candidates for 67 %; the median residual is 1, the mean 2.95 (≈ 1.6 bits), and the maximum 30 for given names, rising to 35 for surnames (Fig. 2 plots the full distribution for both name parts). For contrast, a mask that revealed only the *initial* and the length would leave a median of 71 candidates and uniquely identify under 1 %: it is precisely the disclosure of the leading *half* that collapses the set. The earlier “initial-only” intuition thus understated the leak by about two orders of magnitude.

The Thai surname makes this worse. Under the Surname Act B.E. 2456 (1913), every Thai family must hold a *distinct* surname, and two unrelated people almost never share one [19]; consistent with this, roughly 81 % of Thai surnames are unique to a single bearer, the ten commonest cover only 1.1 % of the population, and the modal surname is rare [20]. A surname is thus

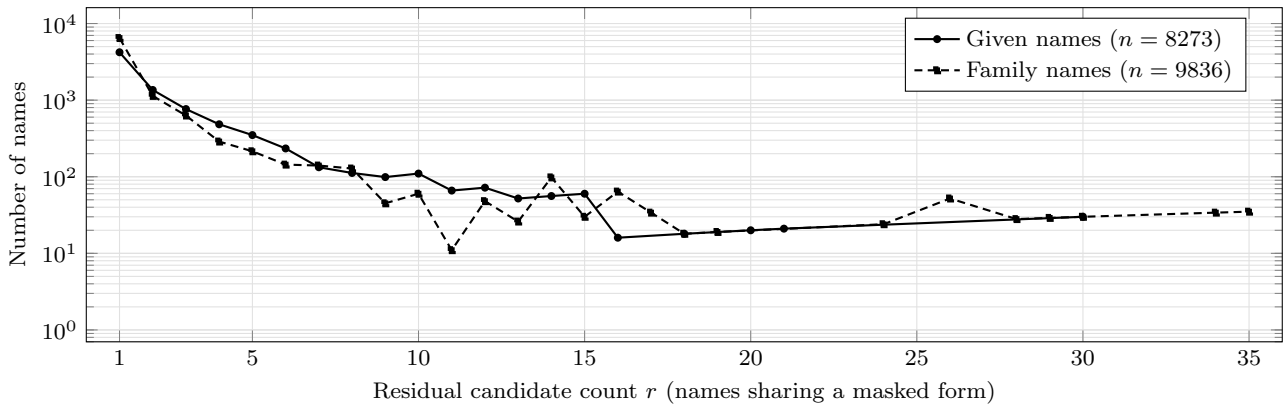
⁴ We deliberately compute on Thai script rather than romanised forms: PromptPay renders recipient names in Thai (§9), and romanisation is many-to-one, which would blur the length and prefix the mask exposes. Character counts and $\lceil L/2 \rceil$ below are therefore over Thai characters.

Table 4 What PayNow’s mask reveals, on ABS’s own published examples.

Registered name	Words	Per-word lengths	Revealed / hidden chars
Chan Shi Hui Jacqueline	4	4,3,3,10	11 / 9
Muhammad Hakeem bin Osman	4	8,6,3,5	13 / 9
Muthu Ramesh Murugan s/o P.Loganathan	5	5,6,7,3,12	17 / 16

Table 5 Residual candidate count left by the ABS mask over 8273 Thai given names and 9836 Thai family names: the share of names whose masked form (length + first $\lceil L/2 \rceil$ characters) matches exactly r names in its corpus. The mask leaves a family name unique more often than a given name.

Residual r	Given name ($n = 8273$)		Family name ($n = 9836$)	
	Share	Cumulative	Share	Cumulative
1	51.0 %	51.0 %	65.8 %	65.8 %
2	16.4 %	67.4 %	11.5 %	77.3 %
3	9.2 %	76.6 %	6.4 %	83.7 %
4–5	10.1 %	86.7 %	5.1 %	88.8 %
≥ 6	13.3 %	100 %	11.2 %	100 %

**Fig. 2** Full distribution of the residual candidate count r left by the ABS mask, on a logarithmic scale (the tail summarised in Table 5). Most names fall at $r \leq 3$, but a thin tail of tightly clustered length/prefix classes reaches $r = 30$ for given names and $r = 35$ for family names. Family names concentrate at $r = 1$ more strongly (65.8 % versus 51.0 %), so the mask leaves them unique more often.

close to a unique identifier before any masking. Applying the same collision computation to a public corpus of 9836 distinct Thai family names [21], the mask leaves a unique surname string for 65.8 % of them (a higher rate than the 51 % for given names), with median residual 1 and mean 2.92 (Table 5). Since a Thai surname is borne, in roughly 81 % of cases, by a single family, a masked surname that resolves to a unique string pins down one family, and the given name then resolves the individual within it. Because the mask acts on each word independently, a full name is uniquely recovered only when *both* its given name and its surname are individually unique. Over the Cartesian product of the two corpora (a space of name *strings*, not a population sample), this holds for $0.51 \times 0.658 \approx 33.6\%$ of given/surname combinations, in agreement with the direct enumeration in `rq2b_joint_fullname.py`. The lower full-name figure is not a sign that masking helps: it reflects the

strict requirement that *both* words be simultaneously unique, and the distribution over all combinations still has a median of two. We report this over distinct name strings, not over the population, and make no population de-anonymisation claim, which would need a joint given/surname frequency distribution we neither hold nor should collect (§12). But the direction is unambiguous, and it is telling that the very examples ABS published to justify the mask use *shared* surnames (common Chinese, Malay, and Indian names), the regime in which masking helps most, whereas Thailand’s near-unique surnames are the regime in which it helps least.

The mask is thus effective against a human skim-reader harvesting a readable name, but weak in Thailand even for that purpose, and, against an adversary who already *holds* a candidate name and need only test $\mu(n) \stackrel{?}{=} m$ (the adversary Sections 5–7 construct), irrelevant everywhere. Masking mitigates display-harvesting;

it does not mitigate oracle-backed confirmation. Quantitatively (Table 5) and structurally, this is the core of our argument that the binding controls are rate limiting and anomaly detection, not display format. Thailand, moreover, applies no masking at all (§9).

9 What Thailand actually discloses

Sections 5–8 are analytical. To ground them we ran the oracle against identifiers the authors themselves hold. PromptPay is opt-in and per-account: the holder must actively *bind* a proxy (mobile number, national ID) to a specific existing bank account, and the name the oracle returns is that bound account’s registered name. Binding national IDs and mobile numbers to accounts the authors hold at two banks (Bangkok Bank; Krung Thai Bank), we queried each proxy from the mobile apps of seven banks spanning state-owned, private, foreign, and Islamic institutions (Table 6). The unit of analysis is the *display policy*, which turns out to be uniform across the ecosystem.

No masking, ecosystem-wide. Every one of the seven querying apps, for every proxy and every bound bank, returned the *full* account-holder name, with no redaction of any kind. The partial-name masking that Singapore adopted in June 2026, and whose residual identifiability we quantified in §8, is simply absent in Thailand. The mitigation is not merely weak here; it is not deployed anywhere in the surveyed set.

Resolution is national, not per-bank. A proxy bound at one bank resolved, with the full name, from all seven apps, including state-owned, private, foreign, and Islamic banks. That institutions of such different type behave identically confirms the threat model’s assumption (§4): each app is a query interface onto one central oracle (operated via the ITMX Multi Proxy Platform), and the display behaviour is fixed by the shared scheme rules, not chosen per bank.

The name comes from the bound account, not a central record. The oracle returns the registered-name string of the account each proxy was bound to at its *originating* bank, so trivial formatting differences (e.g. spacing) simply reflect that bank’s account-naming convention rather than anything about the oracle. The destination bank itself is never displayed: the oracle discloses identity, not banking relationship.

An incidental throttling observation. While exercising the confirmation screen on our own proxy through ordinary back-and-forth navigation, one of the seven apps returned the full name on approximately fifty consecutive resolutions of the *same, authors’-own* proxy within about two minutes, with no throttling, warning, added authentication, or degradation observed. This is a weak, single-app lower bound, not a throttling study; it is consistent with the absence of an aggressive per-session rate limit on that app, but says nothing about limits at higher volumes or on other apps. We did not push further, by design (§4, Ethics); a systematic measurement is left to future work with the operator (§12, item 4).

Scope. These observations establish the policy-level facts (no masking, uniform across seven banks of four institutional types; national rather than per-bank resolution) from the authors’ own accounts only. Beyond the single incidental observation above we make no claim about lookup throttling, and we do not report attack success rates, which our ethical design precludes.

10 Discussion

Why confirmation changes the threat. The SSN-era defence against predictable identifiers was to reduce predictability: randomise issuance, decouple the number from birth data [5]. That defence targets the *prediction* step. An oracle makes prediction almost irrelevant: an adversary need only reach a small candidate set, which structure alone provides, and the oracle supplies the certificate. Reducing predictability raises the cost of forming candidates but does nothing about the confirmation step, because the confirmation lives in a different system (the payment rail) than the one that issues the identifier. Defences chosen for a world without oracles do not transfer to a world with them.

Display versus oracle. Singapore’s response, masking the displayed name, treats the harm as a *display* problem: stop a human from reading a name off a screen. Our collision analysis (§8) and the algebra of the threat model (§4) show the harm is an *oracle* problem: an adversary who already holds a candidate name confirms it by equality test, masked or not. Masking is worth doing against casual display-harvesting, but it is the wrong layer for the adversary that structure-plus-leak produces. Thailand, meanwhile, applies no masking at all (§9), so even that partial measure is absent.

An unavoidable tension. The resolution feature cannot simply be switched off: it prevents misdirected payments and, in the EU, is now legally required. The value

Table 6 Name returned by the PromptPay oracle for the authors’ own proxies. Every combination of bound bank and querying app returned the *full*, unmasked account-holder name. Names inspected with the authors’ consent.

Bound at (originating bank)	Queried from (app)	Name displayed
Bangkok Bank / Krung Thai Bank	Bangkok Bank, Krung Thai Bank, Kasikornbank, TMBThanachart (ttb), United Overseas Bank (Thai), Siam Commercial Bank, Islamic Bank of Thailand	full , unmasked

and the harm are two readings of one function. This is why the actionable lever is not *whether* to resolve but *how often* and *how observably*: controls on the query, not on the display.

Generality and future work. The argument is not specific to Thailand; it applies to any proxy-addressed system with an open resolution step: UPI, PIX, PayNow, and the eurozone’s new Verification of Payee. Thailand is a sharp instance because its identifiers are highly structured and a large leak already exists, but the composition “predictable identifier + confirmation oracle” is general. The *cross-border* linkages now connecting these systems make the composition especially pointed, and here the guarantee is already visibly asymmetric. For PayNow cross-border transfers Singapore masks the payee’s name with asterisks, and corporate (UEN) payees are exempt from the new masking altogether [13]; yet Thailand, which resolves the same proxies domestically with no masking at all (§9), applies no comparable protection. Whether a Thai payee’s name is masked when a Singaporean payer resolves it across the link, and whether the protection a payee enjoys thus depends on which country’s app is querying, is a direct measurement we leave to future work, as it requires cooperating accounts in both jurisdictions.

System by system. The two axes of Table 1 predict where the composition bites. India’s UPI resolves a mobile number or virtual payment address to a registered name; the identifier is semi-structured and widely recorded, so discovery is feasible, though UPI’s signed-intent flows and per-application limits raise the cost of resolving in bulk. Brazil’s PIX is the closest analogue to Thailand: its keys include the CPF, a check-digitated national identifier whose structure shrinks the search space exactly as the Thai national ID does, alongside mobile numbers. Singapore’s PayNow, keyed on the NRIC and mobile number, is the only system to have acted, and it acted on the display layer, whose limits we quantify in §8. The eurozone’s Verification of Payee is the outlier in the safe direction: a match/no-match verdict against a payer-supplied name withholds the candidate set, and keying on an IBAN that is not derived from public data withholds the predictable identifier,

so it denies the adversary both halves of the composition. The lesson generalises beyond payments to any population-scale directory that maps a guessable key to a real name.

11 Recommendations

Our results point to controls on the *query*, not the display:

- **Rate-limit and profile lookups.** An honest payer resolves a handful of new proxies a day; bulk or systematic resolution is anomalous and detectable. This is the control that actually binds the adversary of §4. A recent commentary [14] argued, in the PayNow debate, that lookup limits matter more than display format; our analysis supplies the mechanism behind that claim (an oracle defeats masking but not query controls) and the same intuition appears in the operator’s own rationale for its 2026 change [13].
- **Prefer confirmation to discovery in the interface.** Where feasible, verify a payer-supplied name against the account rather than volunteering the registered name outright: a match/no-match response discloses far less than a full name.
- **Mask, but do not rely on masking.** Partial masking (§8) raises the bar for casual harvesting and is worth adopting (Thailand currently does not) but it must be understood as a display measure, not a defence against oracle-backed confirmation.
- **Treat identifier structure as a privacy parameter.** Where a national identifier embeds a check digit and geographic data, its resolvability against a leak should inform how freely the resolution oracle is exposed.

12 Limitations

Several limitations bound our claims and mark where the strong version of each would require work we deliberately did not do. (1) *Measurement breadth.* The disclosure measurement (§9) spans seven querying apps and two originating banks but only the authors’ own

proxies; it establishes the policy-level facts (no masking; national resolution) robustly across institution types, but by design it cannot measure quantities that vary per *target* rather than per bank, which our own-accounts-only constraint precludes. (2) *Name statistics*. The given-name result (Table 5) is a *direct* computation over a public corpus, not an aggregator estimate; its limitations are the corpus’s coverage (8273 common given names, so rarer forms are under-represented, which if anything *understates* uniqueness) and its Thai-script basis (§8). The *surname* collision figure (§8) is likewise a direct computation, over a separate public corpus of 9836 Thai family names; only the surname *population*-concentration figures (the 81 % unique and 1.1 % top-ten share) still come from an aggregator whose totals romanisation variants inflate, so we lean on those concentration ratios rather than the raw totals. The full-name figure (33.6 % unique, §8) is the product of the two per-word rates under an assumption that given name and surname are statistically independent; Thai naming carries some regional and lineage correlation, so we treat it as an approximation. We report no population de-anonymisation rate for full names, as that would need a joint given/surname frequency distribution we deliberately do not collect. (3) *Leak composition*. The name-less fraction of the leaked corpus is not reported by the source and we do not estimate it numerically; our enrichment claim is argued qualitatively and bounded conservatively. (4) *Throttling*. Beyond a single incidental observation (§9: one app returned the name on ~50 consecutive resolutions of our own proxy in two minutes without throttling), we did not measure rate limiting. Establishing it reliably would require either the operator’s cooperation and logs or generating an abnormal volume of queries against production infrastructure, which we judged inappropriate; the recommendation of rate limiting is therefore prescriptive, and its systematic verification is left to the operator or to future work conducted with their cooperation. (5) *Analysis, not demonstration*. The partial-recovery and composition results (§6, §7) are computed, never executed against real identifiers; we cannot and do not report empirical attack success rates, by ethical design.

Declarations

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interests The authors declare that they have no competing interests.

Ethics approval This study did not involve human participants, human tissue, or personal data about any third party, and therefore did not require review by an institutional review board. All resolution queries reported in Sect. 9 were performed by the authors on payment proxies that the authors themselves own and control, using ordinary consumer banking applications. No identifier belonging to any third party was ever queried, and no enumeration of the identifier space was performed at any point. The analyses in Sects. 5–7 are arithmetic over published parameters and previously published aggregate statistics; no new data about any individual was collected. The name corpora used in Sect. 8 are publicly released, deduplicated lists of name strings, not records about identifiable persons. This design is consistent with the Thai Computer Crime Act B.E. 2550 (§§5 and 7) and the Personal Data Protection Act B.E. 2562 (§§24 and 26). The authors accordingly judge the work in Sect. 9 to be self-experimentation rather than human-subjects research.

Consent to participate Not applicable: the study involved no human subjects other than the authors themselves.

Consent for publication Not applicable: the manuscript contains no data or images identifying any individual other than the authors, who consent to publication.

Data and materials availability The public Thai given-name and family-name corpora used in Sect. 8 are cited [18, 21]; the verified Thai QR / PromptPay standard reference and the computation inputs are released with the code (below). They contain only public parameters and published aggregate statistics: no personal data, no identifier, and no lookup result is included.

Code availability The calculation scripts (`rq4_idspace.py`, `rq2_masking.py`, `rq2b_joint_fullname.py`, `rq5_scale.py`) are released at <https://github.com/mamamind47/promptpay-resolution-oracle>, in keeping with the ethics protocol above.

Author contributions B.S. conceived the study, designed the threat model and the measurement protocol, implemented and ran the computational analyses, performed the self-experiment on the authors’ own accounts, and wrote the first draft of the manuscript. T.T. supervised the work, advised on scope, methodology, and the ethical boundaries of the measurement design, selected the publication venue, and critically revised the manuscript. Both authors read and approved the final manuscript.

Responsible disclosure We characterise the behaviour described in this paper as a design property of a national payment scheme rather than a software vulnerability, and standard coordinated vulnerability disclosure does not apply to it. Three facts support this characterisation. First, the resolution behaviour is a documented, intentional feature of the scheme: the payee-name check exists precisely so that payers can confirm the recipient before authorising a transfer, and an equivalent mechanism is legally mandated for eurozone providers from October 2025. Second, every input to our analysis is already public: the national identifier layout is published by the issuing authority, the QR payload format is published by the scheme regulator, the name corpora are publicly released datasets, and the identifier leak we compose with has been documented in the peer-reviewed literature. Third, we disclose no exploit and no operational detail beyond what any user of a Thai banking application already observes: we ran no queries against third-party identifiers, we performed no enumeration, and we report no attack success rates. There is consequently no secret to withhold, no patch to coordinate, and no window during which disclosure would place account holders at additional risk. What the paper proposes is not a fix to a defect but a change in scheme-level policy, namely query rate limiting and anomaly detection (Sect. 11), which is a matter for public deliberation among operators, regulators, and the research community rather than for private notification. We therefore publish through the ordinary academic channel.

References

1. European Union. Instant payments regulation: Verification of payee obligations (2025). In force for eurozone PSPs from 9 October 2025
2. A. Acquisti, R. Gross, Proceedings of the National Academy of Sciences **106**(27), 10975 (2009). DOI 10.1073/pnas.0904891106
3. EMVCo, EMV QR Code specification for payment systems: Merchant-presented mode, v1.1. Tech. rep. (2020)
4. Bank of Thailand. Policy guideline: Standardized Thai QR Code for payment transactions (2019). FPG 25620084, 17 April 2019
5. W.E. Winkler, Proceedings of the National Academy of Sciences **106**(27), 10877 (2009). DOI 10.1073/pnas.0905722106
6. SpyCloud Labs. What insights can we gain from 1 billion leaked Chinese national ID numbers? <https://spycloud.com/blog/insights-from-leaked-chinese-national-id-numbers/> (2024). Accessed 2026-08-27
7. L. Sweeney, Simple demographics often identify people uniquely. Tech. Rep. Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh, PA (2000)
8. L. Sweeney, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **10**(5), 557 (2002). DOI 10.1142/S0218488502001648
9. A. Narayanan, V. Shmatikov, in *2008 IEEE Symposium on Security and Privacy* (2008), pp. 111–125. DOI 10.1109/SP.2008.33
10. Y.A. de Montjoye, L. Radaelli, V.K. Singh, A. Pentland, Science **347**(6221), 536 (2015). DOI 10.1126/science.1256297
11. B. Reaves, N. Scaife, A. Bates, P. Traynor, K.R. Butler, in *24th USENIX Security Symposium* (2015)
12. R. Kumar, S. Kishore, H. Lu, A. Prakash, in *29th USENIX Security Symposium* (2020)
13. Association of Banks in Singapore. PayNow nickname feature to cease from 6 June 2026 to strengthen protection against impersonation scams. ABS Media Release, 29 April 2026 (2026)
14. D. Rabetti. What PayNow’s alias removal really signals. NUS Business School commentary, The Straits Times, 28 May 2026 (2026)
15. Monetary Authority of Singapore, Association of Banks in Singapore. Joint ABS–MAS response to “what PayNow’s alias removal really signals”. <https://www.mas.gov.sg/news/letters/2026/joint-abs-mas-response-to-dr-daniel-rabetti>, 3 June 2026 (2026)
16. S. Sivakorn, S. Malaivongs, N. Rujiratanapat, International Journal of Information Security (2026). DOI 10.1007/s10207-026-01270-w. Accepted 30 April 2026
17. Department of Provincial Administration (DOPA), Ministry of Interior, Thailand. Meaning of the 13-digit national identification number [in thai]. <https://multi.dopa.go.th/secofdopa/news/cate10/view207> (2014). Accessed 2026-08-27
18. Name Census / Thai Firstname Corpus. Thai given-name frequency lists. <https://huggingface.co/datasets/suchut/thai-firstname-corpus>; <https://census.name/thai-name-database/> (2024). Thai Firstname Corpus (HuggingFace), 8,273 distinct given names, used for the residual computation; the Name Census list reports 8,626. Accessed 2026-08-27
19. Government of Thailand. Surname act, b.e. 2456 (1913) (1913). Requires each family to hold a distinct surname
20. Forebears. Thailand surnames — incidence and frequency. <https://forebears.io/thailand/surnames> (2024). Aggregate estimate; accessed 2026-08-27
21. Korkeat W. Thai names corpus — thai male, female and family names. <https://github.com/korkeatw/thai-names-corpus> (2020). A deduplicated word list of distinct surname strings (9,836 family names), not records linked to individuals; CC BY-SA 4.0; compiled from publicly available web data and 2019 general-election candidate names. Accessed 2026-09-06.