MONTHLY
FEBRUARY 2026

MWEBESA
LAW GROUP

Newsletter

Whats new IN THIS ISSUE

EDITOR'S NOTE -- FEBRUARY EDITION

Dear Esteemed Clients, Stakeholders, and Readers,

To our clients in banking and financial services, try this small experiment. Walk into your server room or open your cloud dashboard, and ask a simple question: what data is sitting here that should have been deleted last year? Now try another: if a regulator walked in tomorrow and demanded to see every piece of personal information you hold on a specific customer, could you show them, quickly, completely, and with confidence?

Now to the rest of the readers, shift your attention to your corporate structure. Ask yourself: who really owns this institution? Not just the names on the share certificate, but the human beings behind the holding company registered in a different jurisdiction. If a lender or a serious investor asked for a clean, simple explanation of your ownership chain, could you give one without long pauses and complicated footnotes?

These are the kinds of questions that keep regulators awake, that derail transactions, and that turn routine audits into existential crises.

Our February edition tackles both.
Our first feature, "Beyond the Checkbox: What banks and financial institutions still get wrong about data, consent, and reporting," is about the gap between ticking boxes and real compliance. We walk through the "consent illusion", the comfortable myth that a signature buried on page 47 of an account opening form equals the "genuine understanding" the law now requires under the Personal Data Protection Act. We examine the "data retention dilemma," where holding onto data "just in case" creates a daily, compounding liability under the PDPA's storage limitation principle. And we look at the specific places where institutions stumble: automated credit scoring, biometric authentication, cross-border cloud storage.

In the end, our message is simple: if you are still treating data protection as a compliance exercise rather than an operational discipline, you are already behind.

Our second feature," The web of control: how companies are owned and controlled through indirect means," asks a different set of questions. In our experience, many business leaders know what they own but cannot clearly answer who owns it, legally, beneficially, and ultimately. We move beyond the simple distinction between "owning" and "operating" to examine the layers of indirect ownership that characterize modern enterprises: holding companies, trusts, nominee arrangements, cross-border structures. This piece is for the founder who wants to protect assets, the investor conducting due diligence, and the board member who needs to know where liability actually rests. Because in an era of beneficial ownership registers and enhanced scrutiny, a structure you cannot clearly explain is a structure that will eventually cost you.

Across both pieces, a single theme emerges: the era of opacity is over. Whether it is opacity about how customer data is used, or opacity about who stands behind a corporate vehicle, the old instinct to obscure, to bury in fine print, to assume no one will look too closely, that instinct is now a liability.

The institutions that will thrive are those that embrace clarity. They design consent mechanisms that actually inform. They build retention schedules that actually delete. They construct ownership architectures that can withstand scrutiny from a regulator, a lender, or a successor.
This February, we invite you to look closely at both your data and your structure. Not because the law demands it, though it does but because trust, in the end, is built on clarity. Thank you for reading, for questioning, and for growing with us.

Happy reading!
The Editorial Team
MWEBESA LAW GROUP

CONTENTS

BEYOND THE CHECKBOX: WHAT BANKS AND FINANCIAL INSTITUTIONS STILL GET WRONG ABOUT DATA, CONSENT, AND REPORTING.

1. INTRODUCTION

The average bank today holds more personal data on a single customer than that customer's family, employer, and closest friends combined. Every swipe of a card, every login location, every bill payment, it all lives somewhere in the vast digital architecture of the financial system. And yet, walk into most bank compliance meetings and you will hear the same comfortable word: "covered." Covered in the privacy policy. Covered in the terms and conditions. Covered at account opening. The checkbox has been ticked, the lawyers are satisfied, move along.

Except the customers are not moving along. They are growing restless. They are starting to ask uncomfortable questions about who saw their transaction history, why they keep getting calls about loans they never applied for, and how long their data will sit on servers they cannot see.

This article is for the people who have to answer those questions. For legal counsels trying to explain to the board why the old way of doing things is suddenly attracting regulatory attention. For heads of risk and compliance who know that somewhere in the bank's systems, data is sitting where it should not be, kept longer than it should be, used in ways the customer never really understood.

The argument here that the checkbox approach to data protection is not just outdated, it is dangerous. And the institutions that continue treating privacy as an administrative formality rather than an operational discipline will find themselves on the wrong side of both regulators and the customers they exist to serve.

2. THE LEGAL LANDSCAPE: MORE THAN A PAPER EXERCISE

Before we talk about what banks and financial institutions get wrong, we need to be clear about what the law actually requires. Because the gap between "what the law says" and "what the institutions hear" is where most of the trouble begins. Tanzania's data protection framework is a living web of interlocking obligations that touch every part of a financial institution's operations.

The Personal Data Protection Act of 2022 sits at the centre. It creates the Personal Data Protection Commission, gives it teeth, and establishes principles that sound simple on paper but run deep in practice: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, security. Words that lawyers nod along to that IT departments struggle to implement.

Then come the regulations of 2023, which turn those principles into concrete requirements. Registration with the commission, appointment of a data protection officer (DPO), quarterly compliance reports, risk assessments before launching anything new and cross-border transfer restrictions. And yes, consent rules that make the old "check the box" approach legally indefensible. But here is where financial institutions face a unique challenge. They are not governed only by data protection law. They are also governed by:

2.1 The Banking and Financial Institutions Act, with its ancient but powerful secrecy provisions that treat customer information almost like confessional secrets.
2.2 The Bank of Tanzania's Financial Consumer Protection Regulations, which specifically address how customer data should be handled, shared, and protected.
2.3 The Anti-Money Laundering Act, which demands ten years of record-keeping and creates a instinct to hoard data "just in case."
2.4 The Credit Reference Bureau Regulations, which create entire databases of sensitive financial information with their own access a and correction rules.
2.5 The Microfinance Act and its accompanying regulations, extending these obligations to institutions serving customers who may have the least power to protect themselves.

On paper, this framework is clear however in practice, it creates a kind of regulatory vertigo. Banks are pulled in different directions. The AML people say keep everything for ten years. The data protection people say delete what you no longer need. The business people say we might need this for future products. The lawyers say we should probably keep it to be safe. And so, the data stays. Indefinitely. Accumulating. Growing stale. Becoming a liability that no one has fully priced. The regulators are watching this. They know that compliance on paper is not the same as compliance in practice. And increasingly, they are acting on that knowledge.

3. WHERE INSTITUTIONS GO WRONG

3.1 The Consent Illusion

Let us talk about consent. Specifically, about what banks call consent and what the law actually requires. The typical account opening process is a masterclass in what data protection experts call "consent illusion." The customer sits down, is handed a sheaf of papers, and told to sign here, here, and here. Somewhere in those pages, buried under sections titled "General Terms and Conditions" or "Privacy Notice," are sentences authorizing the bank to use the customer's data for purposes the customer cannot possibly absorb in that moment. The bank calls this consent. The law calls it something else.

Section 23 of the Personal Data Protection Act requires that before any data is collected, the customer must be fully aware of the specific purposes. Regulation 25 goes further, demanding that customers have an "autonomous right to freedom to control his personal data" and possess a genuine "understanding of what he consented to." Read that again. Genuine understanding. Not a signature, not a checkbox, not an "I agree" click. Genuine understanding.

This is a fundamental shift in how consent operates. Under the old model, consent was a transaction: sign here, we can use your data. Under the new model, consent is an ongoing relationship: we can only use your data for things you actually understood you were agreeing to, and you can walk away at any time.

The law even requires a "simplified means to withdraw consent." No explanations. No charges. No friction. Just a clean, easy exit. How many institutions have built that? How many mobile apps have a button that says "stop using my data for marketing" that actually works? How many websites make it as easy to withdraw consent as **it was to give it?**

3.2 The Data retention dilemma

Here is another scenario that plays out in institutions across the country every single day. Someone applies for a loan, the institution runs checks, reviews the application, and says no. The file is closed; the applicant moves on but the data stays. It stays because the bank is afraid of the Section 32Anti-Money Laundering Act, which requires records to be kept for ten years after a transaction is completed or a business relationship ends. The compliance officer reads this and thinks: better keep everything, just to be safe.

But here is what that compliance officer missed. Section 3 of the AML Act defines a business relationship as an arrangement involving the establishment of a customer account or the provision of services through ongoing transactions. A rejected loan applicant never received a service. No account was opened. No ongoing relationship was formed. The AML retention rule does not apply.

Yet the data sits there, year after year becoming a target for hackers. Becoming a liability on the balance sheet. Becoming evidence, someday, of an institution that kept data without justification. This is digital hoarding and it carries real consequences. If unauthorized data sits on your systems and you know it is there but do nothing about it, you are not just committing a past violation. You are committing a new violation every single day that data remains. The math is a small fine multiplied by 365 days which becomes a very large fine. A reputational hit multiplied by years of neglect becomes an existential crisis.

3.3 Automated Credit Scoring

Digital lending is fast. Algorithms can approve or reject applications in seconds. Customers love the speed and institutions love the efficiency. But the law requires something else, when decisions that significantly affect a person's financial life are made solely by machines, customers have rights. They have the right to be told that a machine made the decision. They have the right to ask for human review. They have the right to understand how the algorithm reached its conclusion.

However, how many banks using automated scoring have actually built those rights into their systems? How many loan rejection letters explain that the decision was automated and explain how to request reconsideration? The law requires it but practice rarely delivers.

3.4 Biometric Authentication

Fingerprints and facial scans are also very convenient. They are also, in the eyes of the law, sensitive personal data. This is not the same category as your name or your address. It is a higher category, attracting stricter rules. Sensitive data cannot be collected through generic terms and conditions. It requires prior, explicit, written consent. It requires the customer to understand exactly what they are giving and why. It requires a clear mechanism for withdrawal. The institution that asks for a fingerprint scan without explaining these things is building on shaky ground

3.5 Cross-Selling and Marketing

Analysing transaction patterns to offer new products is good business. If someone spends heavily on travel, offering them a travel credit card makes sense. If someone has a large savings balance, offering investment advice is logical. But the law gives customers control over how their data is used for marketing. They can say no. They can demand that their data

not be processed for direct marketing, and the institution must provide a clear, accessible way to exercise that right.

A checkbox buried in account opening documents does not meet this standard. A customer who cannot figure out how to stop marketing calls is a customer whose rights have been violated, even if the marketing itself is legal.

3.6 Credit Reference Bureau Checks

Credit reporting is essential to modern lending. But it involves something the regulations identify as potentially high-risk: linking multiple datasets about an individual's financial activities. Transaction data from the bank, credit history from the bureau, payment records from other lenders. All combined into a single profile. Because financial transaction data is sensitive personal data, this aggregation requires clear information and explicit consent. The customer must understand that their data will be shared, combined, and analyzed. The customer must agree to this, not as part of a general bundle, but as a specific, informed choice.

3.7 Cross-Border Cloud Storage

Modern banking runs on the cloud. Servers in different countries. Data centers on different continents. Backups in locations the customer has never heard of. The law cares about this. Transferring personal data outside the country is strictly regulated, especially when the destination does not provide adequate protection. In many cases, these transfers require explicit consent from the data subject.
A privacy policy that mentions "international service providers" in paragraph 47 does not satisfy this requirement. The customer must be properly informed and must explicitly consent to the data transfer. Anything less is a violation waiting to happen.

4. RECOMMENDATIONS: MOVING BEYOND THE CHECKBOX

So what does "beyond the checkbox" actually look like in practice? For legal counsels and heads of risk and compliance, it means a fundamental shift in how data protection is understood and operationalized.

4.1 First, stop treating data protection as a compliance exercise. Compliance is about meeting minimum standards. Data protection, properly understood, is about building trust. The difference matters. Compliance asks "can we prove we followed the rules?" Trust asks "does the customer believe we handled their information responsibly?" The second question is harder to answer, but it is the one that determines whether customers stay or leave.

4.2 Second, embed transparency into products, not policies. A privacy policy is a legal document. Transparency is a product feature. It means designing interfaces that actually inform customers, in plain language, about what will happen to their data. It means building consent mechanisms that allow genuine choice, not just acceptance. It means creating withdrawal processes that work as smoothly as the original sign-up.

4.3 Third, audit what you actually hold. Most institution have only a vague idea of what data sits where. Legacy systems, old backups, spreadsheets on shared drives. The first step to fixing data retention problems is knowing what data exists. The second step is asking, for each piece of data, whether retention is actually justified. The third step is building processes to delete what cannot be justified, securely and permanently.

4.4 Fourth, match lawful bases to processing activities. Not everything requires consent. Not everything can be justified by legitimate interest. For each significant processing activity, credit scoring, marketing, biometric authentication, cross-border transfer, ask the hard question: what is the lawful basis, and can we prove it applies? If the answer is unclear, the risk is real.

4.5 Fifth, empower your Data Protection Officer. A DPO who cannot act is a DPO who cannot protect you. The role needs authority, resources, and access to decision-makers. It needs to be involved when new products are designed, not called in after something goes wrong. It needs to be heard when it raises concerns, not tolerated until the quarterly report is filed.

4.6 Sixth, build for withdrawal. Consent that cannot be withdrawn is not consent. Build systems that allow customers to change their minds. Build interfaces that make withdrawal as easy as giving permission. Build processes that ensure withdrawal is actually implemented, across all systems, without delay.

5. CONCLUSION

The era of treating data protection as a legal afterthought is over. What many banks and financial institutions continue to get wrong is not simply the law, it is the mindset. Privacy is still too often viewed as a document to file, a policy to upload, or a consent box to tick.

In reality, it is an operational discipline that must live inside systems, teams, and product design decisions every single day. It is about building architectures that respect customer choices. It is about creating processes that actually delete data when retention periods expire. It is about designing interfaces that inform rather than obscure.

The institutions that will thrive in the next decade are not the ones with the longest privacy policies or the most impressive compliance binders. They are the ones that quietly embed privacy into their architecture, empower their Data Protection Officers, and treat customer data with the same seriousness they treat customer money. Because in today's financial ecosystem, trust is no longer built only on interest rates and uptime. It is built slowly, invisibly, and decisively on how responsibly you handle the data people cannot afford to have exposed.

THE WEB OF CONTROL: HOW COMPANIES ARE OWNED AND CONTROLLED THROUGH INDIRECT MEANS

1. INTRODUCTION

At first glance, the ownership of a company appears to be a matter of public record: a list of shareholders and a board of directors, filed with a registrar and available for anyone to see. Yet, in the complex reality of modern corporate practice, this registry often tells an incomplete story. It reveals who holds the legal title, but it frequently obscures the identity of the person who truly directs decisions or the one who ultimately enjoys the economic benefits generated by the enterprise.

Corporate law itself acknowledges and permits this distinction. It creates a crucial separation between the legal owner of a share, the individual with the authority to vote it, and the beneficiary who reaps its rewards. This is not an accident or a loophole, but a feature of the legal landscape designed to accommodate valid and strategic business purposes. The motivations are varied and legitimate: a passive investor may seek protection from liability by holding shares through a holding company; a founder may desire the flexibility to attract talent with different classes of shares; a prominent business owner may prize privacy to shield their holdings from public view; and a family may seek to ensure the continuity of an enterprise across multiple generations through carefully structured trusts.

This separation of legal title, operational control, and economic benefit is the essence of indirect ownership. It is the mechanism by which influence and value flow not in a straight line, but through a deliberate chain of intermediary entities. While these structures can be misused to obscure illicit activity, their primary purpose is far more constructive. This article will explore how sophisticated investors and enterprises can lawfully leverage these frameworks to foster collaborative ventures, optimize tax efficiency within the bounds of the law, and protect hard-won capital. We will dissect the primary mechanisms of indirect ownership, from holding companies to trusts and partnerships, and analyze the strategic motives

behind them. Ultimately, our goal is to provide a clear analytical framework for understanding these complex structures, ensuring they remain tools for legitimate enterprise that maintain the essential alignment between legal form, operational authority, and economic reality.

2. THE CORE CONCEPT: DEFINING AND DECONSTRUCTING INDIRECT OWNERSHIP

To analyse the intricate architectures of corporate control, we must first establish a clear understanding of the foundational concept upon which they are all built. This requires moving beyond the intuitive notion of ownership and embracing a more nuanced, layered perspective.
At its simplest, ownership can be understood as existing on a spectrum defined by proximity. Direct Ownership is the most transparent form. It exists when a natural person or a legal entity holds shares, and the accompanying voting rights, in a company directly, in their own name. If "Jane Doe" is listed on a company's shareholder register as the owner of 1,000 shares, she is a direct owner. The line from the individual to the asset is immediate and unbroken.

Indirect Ownership, by contrast, introduces intermediaries. It is an ownership interest in an entity that is held through one or more intermediate entities. The legal title to the shares is registered in the name of the intermediary, but the ultimate economic benefit and, often, the power to direct how those shares are voted, resides further up the chain. If "Jane Doe" owns 100% of "Doe Holdings Ltd.," and "Doe Holdings Ltd." owns 1,000 shares in "Target Company Inc.," then Jane Doe is the indirect owner of those shares in Target Company Inc. The line now has a crucial link: Jane -> Doe Holdings -> Target Company. This layered approach creates what is commonly referred to as a chain of control or an ownership chain. Visualizing this chain is essential to understanding how influence and value flow through a corporate group.

Consider a simple illustration:

[Ultimate Owner] *(e.g., a family, a founder, an investment fund)*

↓ (owns 100%)

[Intermediate Holding Company] *(e.g., Family Holdings S.A.)*

↓ (owns a controlling stake, 60%)

[OpCo / Target Company] *(The operating business of interest)*

In this structure, the Ultimate Owners have no direct legal claim on the assets of the Target Company. Legally, the Target Company is owned by the Holding Company. However, because the Ultimate Owners control the Holding Company, they exercise de facto control over the Target Company and are entitled to its economic benefits, which flow back up the chain in the form of dividends.

To navigate these structures with precision, a shared vocabulary is indispensable. Three terms are particularly critical:

- **Ultimate Beneficial Owner (UBO):**
This is perhaps the single most important concept in the entire discussion. The UBO is the natural person (a real, living individual) who ultimately owns or controls a legal entity or arrangement, such as a company, trust, or foundation. They are the "end of the line" in the ownership chain, the principal on whose behalf a transaction is being conducted. Identifying the UBO is the central goal of modern transparency regulations, as it pierces the corporate veil to reveal the human being who truly enjoys the benefits of ownership and exercises ultimate control.

- **Intermediary / Holding Company:**
This is any entity that sits between the UBO and the target company of interest. Its primary purpose may be to hold and manage investments in other companies, rather than to conduct its own operational business. Holding companies are the building blocks of indirect ownership structures, used to create layers, isolate risk, and achieve strategic objectives.

- **Subsidiary and Parent:**
These terms describe the directional relationship between entities in the chain. A subsidiary is a company that is controlled by another company. The controlling company is referred to as its parent (or sometimes a holding company if its primary function is ownership). This parent-subsidiary relationship can repeat itself many times: a company can be a subsidiary of a parent, which is itself a subsidiary of a larger parent at a higher level in the pyramid.

With these foundational concepts established, we can now turn our attention to the specific mechanisms through which indirect ownership is constructed. We will explore the most common structures, from the leverage of pyramids to the privacy of trusts, and analyze how they function in practice.

3. THE MECHANISMS: COMMON TYPES OF INDIRECT OWNERSHIP STRUCTURES

With an understanding of the core concepts, we can now examine the specific legal mechanisms through which indirect ownership is constructed. Each structure represents a distinct answer to the question of how to separate legal title from beneficial enjoyment, and each carries its own unique balance of strategic advantage and inherent risk.

3.1 Holding Companies

The holding company structure is perhaps the most fundamental and widely used form of indirect ownership. It serves as the basic building block for corporate groups of all sizes. The setup is that a parent company, often called a holding company is created with the primary purpose of holding stock or assets in other businesses. This holding company then establishes or acquires subsidiary companies, which it owns either wholly or through a controlling stake. These subsidiaries may, in turn, hold specific properties, operate distinct business segments, or exist as further holding companies in their own right.

From the perspective of a public company registry, the picture is deliberately incomplete. The registry will list the holding company or the immediate intermediary as the direct shareholder of the target company. If that holding company is incorporated in a different jurisdiction, a common practice for tax and privacy reasons, the local registry captures only its domestic segment. This fragmentation of information across borders effectively obscures the ultimate natural person from immediate public view.

The holding company structure offers a compelling array of advantages. It enables centralized strategic management while preserving the legal and financial independence of each subsidiary. This separation creates a powerful risk diversification mechanism: if one subsidiary faces a

lawsuit, insolvency, or regulatory sanction, the parent company's other assets, and the broader corporate group are generally shielded from liability. Additionally, this structure facilitates sophisticated tax planning, efficient asset protection, and streamlined mergers and acquisitions, as entire business lines can be bought or sold through the transfer of subsidiary shares.

These benefits do not come without cost. Layered subsidiaries introduce significant operational complexity, accompanied by high administrative, legal, and compliance expenses. Each entity must maintain its own corporate records, file separate returns, and observe distinct formalities. Furthermore, multi-layered decision-making can create communication delays and dilute accountability, as responsibility for any given action may be diffused across multiple entities and jurisdictions.

3.2 Trusts

Trusts represent a different philosophical approach to indirect ownership. Rather than creating a chain of corporate entities, they rely on fiduciary relationships and contractual agreements to separate legal control from beneficial enjoyment.

Through a legal trust deed, assets or company shares are transferred to a trustee. This party then holds and manages the property not for their own benefit, but on behalf of the designated beneficiaries (in a trust). The trustee holds legal title and exercises managerial authority, while the economic benefits flow to others.

Company registries typically record only the trustee as the legal owner of the shares. Unless the jurisdiction has enacted robust Ultimate Beneficial Owner disclosure rules, a growing but still far from universal trend, the actual beneficiaries remain entirely absent from the public record. This opacity is one of the primary attractions of these structures.

The flexibility of trusts and partnerships is their defining characteristic. They permit highly customized income and profit distribution arrangements, making them ideal vehicles for estate and succession planning. A founder can ensure that a business remains within a family for generations while professional trustees manage its affairs. They also provide efficient asset management and can shield wealth from potential legal claims or creditors, subject to proper structuring and compliance.

However the very flexibility that makes these structures attractive also creates their greatest vulnerability: regulatory scrutiny. If a trustee does not exercise genuine independent fiduciary judgment, but instead acts merely as an administrative front taking orders from an undisclosed beneficiary, regulators may recharacterize the entire arrangement. What was intended as a legitimate trust can be treated as an illicit concealment tool, exposing all parties to serious legal and reputational consequences. The distinction between legitimate fiduciary arrangement and sham is a matter of substance, not form.

3.3 Investment Funds

The rise of institutional investment has made fund structures one of the most pervasive forms of indirect ownership in modern capital markets. Private equity firms, mutual funds, and hedge funds collectively own significant portions of publicly traded companies and an even larger share of private enterprise.

In this case, Investors pool their capital into a fund vehicle, which is typically structured as a limited partnership or a similar pass-through entity. The fund's professional managers then deploy this collective capital to acquire real estate, assets, or shares in various target companies. The investors become limited partners or beneficial owners of the fund, but have no direct relationship with the underlying portfolio companies.

The investment fund itself or, more precisely, its management vehicle or a designated holding entity, appears on the corporate registry as the legal shareholder of the target company. The individual investors, whose capital ultimately funds the investment, are completely absent from the target company's public records. They are invisible to the market, to other shareholders, and to the company's management.

For investors, funds offer two compelling advantages. First, they provide significant risk diversification, allowing individuals to spread their capital across dozens or hundreds of underlying assets with a single investment. Second, they grant access to professional expertise; institutional managers can actively monitor portfolio companies,

engage with management, and drive value creation far more effectively than dispersed individual minority shareholders. Empirical evidence suggests that firms with substantial institutional ownership often experience superior performance.

However, this separation of ownership from control creates an agency problem. Individual investors surrender all day-to-day decision-making power over the specific assets held by the fund. They are passive beneficiaries of whatever decisions the fund managers make. Moreover, fund managers face potential conflicts of interest: they may prioritize maintaining lucrative relationships with corporate executives, who can direct business to the fund's other divisions over challenging management to maximize shareholder value for the fund's own investors.

3.4 Pyramidal and Multi-Tiered Structures

The most sophisticated and most opaque forms of indirect ownership involve the deliberate layering of multiple entities to create pyramidal control structures. These arrangements combine direct and indirect holdings through tiers of pass-through entities to achieve maximum leverage and minimum visibility.

In this scenario, an investor constructs a pyramid of ownership, holding a controlling stake in a top-tier entity, which in turn holds a controlling stake in a lower-tier entity, and so on down the chain. Simultaneously, the investor may also hold a small direct stake in the target company at the bottom. Through the creative use of Limited Liability Companies, partnerships, and other pass-through vehicles, the investor's total economic interest in the target may be modest, while their effective control is absolute.

To an auditor or public registry, the controlling shareholder may appear to hold only an insignificant direct stake, perhaps three or four percent making them look like a minor investor. The true extent of their control is buried deep within the complex web of intermediary partnerships and holding companies. Unravelling this web requires sophisticated link analysis and access to information across multiple jurisdictions, a task that often exceeds the resources of ordinary market participants and regulators.

Pyramidal structures allow an owner to exercise top-down operational control over a vast commercial empire without committing the capital that would be required for full direct ownership. This leverage multiplies the founder's influence. Additionally, pass-through tiering enables groups of investors to combine resources for massive undertakings, such as real estate development or infrastructure projects without the administrative burden of formal corporate taxation, as tax liabilities pass through directly to the individuals.

These structures are however subjected to the highest level of scrutiny from tax authorities, anti-corruption enforcers, and financial intelligence units. Their extreme opacity makes them attractive vehicles for abuse. Controlling shareholders have been known to exploit pyramidal structures to hide their identities and engage in abusive Related Party Transactions, secretly extracting wealth from operating companies for personal benefit while appearing to be mere minority investors. For compliance professionals and regulators, tracing the true Ultimate Beneficial Owners through these structures requires extensive due diligence, cross-jurisdictional monitoring, and a willingness to follow the paper trail wherever it leads.

3.5 Nominee Shareholdings

This mechanism is perhaps the most direct method of separating legal title from beneficial ownership, as it involves a formal, contractual agreement to hold shares on someone else's behalf. A natural person or legal entity (the nominee) holds shares in a company on behalf of another person (the beneficial owner). This relationship is typically governed by a nominee agreement, which legally obligates the nominee to act in accordance with the beneficial owner's instructions, particularly on how to vote the shares and to whom to pay any dividends.

The company registry will list the nominee as the legal shareholder. The name of the true beneficial owner appears nowhere on the public record. This is why nominee arrangements are a primary vehicle for those seeking privacy or, in more problematic cases, anonymity for illicit purposes.

The primary benefit is privacy and asset protection. It allows high-profile individuals to shield their ownership from public scrutiny, competitors, or potential litigants. It can also simplify administrative processes for groups of investors who wish to consolidate their voting power under a single representative.

The risks are substantial and primarily regulatory. Nominee arrangements are a major focus of anti-money laundering (AML) and counter-terrorist financing (CTF) efforts worldwide. If the nominee is merely a "straw man" with no genuine independence and the arrangement is used to conceal criminal activity, both the nominee and the beneficial owner can face severe legal penalties. The key legal test is often whether the nominee exercises any genuine independent judgment or simply follows orders.

4. THE "WHY" AND THE "SO WHAT": STRATEGIC MOTIVES AND THEIR IMPLICATIONS

Having dissected the primary mechanisms of indirect ownership, we must now confront two essential questions. First, why do sophisticated actors go to the considerable trouble and expense of constructing these layered structures? Second, so what? What are the consequences of these structures for the various stakeholders who interact with them, such as regulators, minority shareholders, creditors, and the public?

4.1 The strategic motives: Why layer ownership?

The decision to structure ownership indirectly is rarely accidental. It is a deliberate choice driven by one or more of the following objectives:

4.1.1 Control with reduced capital allows founders to retain authority over vast enterprises while raising external funds, a family that owns 51% of a holding company, which owns 51% of an operating company, effectively controls that operating company with just over 25% of its equity.

4.1.2 Risk mitigation ensures that the liabilities of one venture whether from litigation, contract breaches, or insolvency, do not threaten an entire portfolio; each subsidiary functions as a legal firewall.

4.1.3 Tax optimization, pursued within legal boundaries, preserves capital for reinvestment by situating holding companies in favourable jurisdictions and utilizing pass-through entities to avoid double taxation.

4.1.4 Privacy shields individuals and families from competitors, activists, and opportunistic litigation, allowing high-profile owners to operate without unwanted scrutiny.

4.1.5 Regulatory arbitrage permits navigation around conflicting legal regimes, enabling enterprises to access favourable protections or qualify for local investment incentives.

4.1.6 Succession planning ensures that family enterprises survive the transition between generations by separating economic benefits, which can be distributed among heirs, from operational control, which can be vested in trusted stewards. Each motive reflects a genuine business need, and none is inherently improper.

4.2 The Implications: Consequences for stakeholders

Yet these same structures produce unavoidable consequences for the broader ecosystem in which they operate.

4.2.1 For regulators and governments, layered ownership creates a transparency deficit that hampers tax collection, enables money laundering, and obscures the financing of crime. When ownership is buried behind multiple entities across multiple jurisdictions, authorities cannot easily identify who controls an enterprise or who should be held accountable for its actions. The global push for beneficial ownership registers and cross-border information sharing represents a direct response to this challenge.

4.2.2 For minority shareholders, layered ownership, particularly in pyramids, creates powerful incentives for tunnelling, where controlling shareholders extract value at their expense. Because a controller's cash flow rights are diluted by each layer of the pyramid, the temptation to divert profits through related-party transactions intensifies.

4.2.3 For creditors and investors, opacity complicates risk assessment. A lender evaluating a subsidiary cannot assess it in isolation; they must understand the entire web of intercompany obligations and potential cash flows, increasing the cost and complexity of due diligence.

4.2.4 For the enterprise itself, diffuse accountability can paralyze decision-making and erode governance. When responsibility is scattered across a chain of entities, managers may receive conflicting directives, and boards may struggle to discern whose interests they serve.

4.2.5 And for the public, the perception that wealth can be hidden behind corporate veils erodes trust in the market system itself. When the public reads of corruption scandals, tax avoidance schemes, or anonymous shell companies used to move illicit funds, the cumulative effect is a cynicism that undermines confidence in the rule of law. The legitimate structures designed for privacy and efficiency become, in the public mind, synonymous with secrecy and abuse.

5. CONCLUSION

What emerges from this analysis is that ownership is rarely what it appears to be. The person named on a shareholder register is often a mere placeholder, a single visible node in a chain that leads elsewhere. Behind the holding company lies another holding company. Behind the trustee lies a beneficiary who never appears in any public record. Behind the nominal 3% shareholder lies a pyramidal structure that vests them with effective control of an entire enterprise.

This layered reality exists for reasons that are, in themselves, perfectly reasonable. The business owner who separates assets into distinct subsidiaries is not evading accountability; they are practicing prudent risk management. The family that places its enterprise in a trust is not hiding from scrutiny; they are planning for generations yet unborn. The founder who retains control through a pyramidal structure is not defrauding investors; they are preserving the vision that built the company. The motives matter, and in most cases, they are legitimate.

But legitimacy does not dissolve consequence. Every layer in an ownership chain is also a barrier to transparency. Every intermediary that stands between a beneficiary and their asset is also a potential shield for misconduct. The same structures that protect a family's privacy can protect a money launderer's identity. The same leverage that multiplies a founder's control can facilitate the expropriation of minority shareholders. The same complexity that enables sophisticated tax planning can defeat the efforts of regulators to enforce the law. These are not bugs in the system. They are features, and they have costs.

The global response, beneficial ownership registers, enhanced due diligence, cross-border information sharing, is an attempt to rebalance the equation. Not to eliminate indirect ownership, which would be impossible, but to ensure that opacity is no longer the default. The direction of travel is that the link between legal form and economic reality must be traceable. For those who construct and operate within these structures, the question is no longer whether your structure is legal but whether it can withstand the light. Because in an era of increasing transparency, the only sustainable approach is to ensure that your legitimate need for privacy does not resemble, even accidentally, the illegitimate desire for concealment. Form and substance must align. And every link in the chain, however useful, must be one you are prepared to explain.

MWEBESA
LAW GROUP

DAR ES SALAAM (HQ)

House No. 113, Plot No. 948,
Chole Road, Masaki
P. O. Box 23077
Dar es salaam, Tanzania

ZANZIBAR BRANCH

Block 024, Plot No 55
Mbweni Road, Mazizini, Unguja
Zanzibar, Tanzania

For more information:

Phone: +255 767 348 716 / +255 742 812 125
+255 716 955 304

Email: info@mwebesalaw.co.tz

www.mwebesalaw.co.tz

MWEBESA LAW GROUP