Moving from Identifier to Identity for Researchers

By TIM LLOYD APR 21, 2026

AUTHORS | ETHICS | EXPERIMENTATION | INFRASTRUCTURE | INNOVATION | POLICY | RESEARCH | RESEARCH INTEGRITY | TECHNOLOGY

Editor's note: Today's post is by Tim Lloyd, a member of STM's Researcher Integrity "Task and Finish" group. Tim is also the founder and CEO of LibLynx, a company providing Identity, Access & Analytics solutions for online resources.

The Identity Verification Gap

Most editorial platforms treat identity as simply an identifier (commonly an email address) that lets the platform uniquely identify an individual and associate them with their various roles and activities. Some platforms might confirm ownership of that email address with a link to click on, but even that doesn't actually confirm that you are who you say you are — it simply proves you control it.

This is in stark contrast to corporate platforms, many of which adopt a Know Your Customer (KYC) approach to identity verification that is evolving into increasingly sophisticated risk management frameworks. These rigorous processes are designed to confirm who someone actually is — before granting them access. It's also in contrast to many scholarly publishing platforms, where more modern authentication technologies, like federated authentication, can verify a user's identity and institutional entitlements before granting access. Publishers invest a lot of cost and effort into protecting access to content because it's essential for paywalled business models.

Editorial platforms don't get the same treatment, but they aren't just an obscure backend tool — they're the gateways to our publishing workflows. And when you don't control the gateway to your platform, anything can pass through undetected.

Why Editorial Platforms Were Designed for Trust, Not Verification

So, why does the gap exist between how we manage identity in editorial vs publishing platforms?

The simple answer is that, until relatively recently, there was little benefit in using fraudulent identities for submissions and reviews.

As outlined nicely in a recent *Scholarly Kitchen* article, "The Evolution of the Editorial Office: From Kitchen Tables to Global Infrastructure," editorial platforms grew out of physical editorial offices, with manual and relatively informal processes. When those processes moved online, they largely replicated physical workflows. Identities powered online accounts, acting as a digital filing cabinet for a user's submissions and reviews. Even as editorial systems professionalized and grew in complexity, the underlying assumption remained that people could be trusted to say they are who they are.

What changed was a series of powerful trends over the last decade: globalization, open access publishing models, greater system automation, and, most recently, generative AI. Fueled by academia's publish or perish culture, we entered a world where the cost of creating fraudulent research fell as the incentives to publish it rose.

Our community started to recognize the research integrity threat many years ago, but so far, efforts have almost exclusively focused on the integrity of the content. A growing ecosystem of tools help editorial teams detect plagiarism, manipulated images, fabricated/AI-generated text, inappropriate authorship, citation manipulation, and problematic data. But these remain downstream of a bigger problem: the integrity of the identities involved in authoring, reviewing, and editing submissions.

In late 2023, The International Association of Scientific, Technical, & Medical Publishers (STM) convened a Researcher Integrity "Task and Finish" group (of which I'm a member) to investigate this issue. The group published an initial report on the central role of digital identity in research integrity in October 2024 ("Trusted Identity in Academic Publishing"), followed in March 2025 with a proposed Researcher Identity Verification Framework, which has been supported by numerous presentations across a variety of industry events.

While these initiatives reflect progress, relatively little has changed to date. Most editorial platforms continue to accept personal emails as proof of identity, and few, if any, checks are put in place to verify identity. At the same time, we're collectively pouring money and effort into adding content integrity checks later on in the submission process. Why haven't we added more locks to our front door?

Why Researcher Verification is Complex

As with much of life right now, the reasons why we're not collectively investing more in researcher verification are complex.

Complexity: As submissions have globalized, so has the diversity of researcher experiences. Researchers are more likely to come from institutions that aren't part of the existing research and education identity federations. We have more researchers who choose not to register organizational email addresses or are independent scholars without an institutional affiliation. As access to publication expands, more researchers (including early-career researchers) have limited publication histories to rely on. We need to ensure that verification doesn't become a barrier to genuine contributors.

Inertia: Our industry has prided itself on taking the long view, approaching decision-making with studied consideration. While this has many positive aspects, it makes us susceptible to stagnation during periods of rapid change. And rapid change is exactly what's happening to the publishing ecosystem. We're not recognizing and reacting fast enough to the research integrity risks posed by identity fraud.

Technology adoption further compounds the problem. As editorial platforms have become exponentially more complex, so has the effort and cost involved in maintaining them. We've become reliant on a smaller number of providers, who themselves are facing a greater burden of added complexity. In turn, these providers feed a large community of smaller publishers who lack an independent ability to upgrade their editorial workflow. The result is relatively few large container ships that take a long time to turn.

Focus: Whether it's the research and institutional funding climate, AI upending traditional processes, or the struggle to find the staff (reviewers) to support workflows, editors have a lot to think about. The plethora of research integrity tools focused on content checks makes it easy to address that symptom, but can potentially waste a lot of money if we don't also check those who submit the content. It can feel like endlessly mopping the floor rather than fixing the burst pipe.

Implementation: While we can borrow some approaches from platform authentication (e.g., federated authentication; domain verification), making them work within an editorial environment requires retooling, and they won't work for everyone. Other ideas, like using trust markers or government identity documents, are conceptual and need research and testing to understand how they work in practice. Publishers also vary widely in terms of the risks they face from identity fraud (for example, medical research vs. art history), so there is no one-size-fits-all approach. This is why the STM recommendations propose a framework, not a blueprint for success or an implementation plan.

How to Address the Researcher Verification Gap

Rather than treating researcher verification as a large, one-time investment, we propose a series of incremental improvements that steadily reduce the opportunity for identity fraud. An incremental approach allows our community to tackle the low-hanging fruit first and manage the expectations of researchers so that we minimize the risk of deterring valid submissions.

It's important to bear in mind that the vast majority of fraudulent activity is not the work of devious individual researchers, but rather driven by illegal enterprises working in the shadows and operating at scale, such as paper mills. These enterprises rely on low-cost and highly automated processes that can cheaply generate new identities and research to pump through editorial workflows. Even small amounts of additional cost and/or friction can help to make those processes unprofitable and effectively turn off the taps.

For example, it's essentially costless to mint new Gmail identities and script bots to respond as if the address is managed by a real person. But add the requirement for that email address to be linked to a verifiable human identity, and suddenly both the cost and transparency increase a lot. Simple improvements that editorial platforms can make include:

Validate ownership of email addresses: Stop trusting users on the basis of opaque webmail addresses alone. If your editorial platform doesn't already do this, then add a step to require users to click to enter a one-time code (or click on a link) sent to that email address. Ideally, this should be done periodically to ensure ongoing control. This prevents users from registering an institutional email address that they don't actually own, or continuing to use an email address that they no longer control, e.g., they no longer work at that organization.

Incentivize registration of organizational emails (where possible): Identity fraud is much harder when the email domain is managed by a known organization, such as a research institution. Incentivizing researchers to verify with an organizational email address (or other mechanisms for identity verification) reduces the risk for publishers. While unaffiliated researchers won't have organizational emails to register, many scholars simply choose personal email addresses for simplicity, especially when they are affiliated with multiple organizations. Incentives can be as simple as streamlining future login, allowing greater personalization of their submission system account, or adding visual validation to their publication history, such as LinkedIn's verification checkmark.

Validate institutional affiliation (where possible): Not all organizational emails validate a user's research credentials, so an additional step is to confirm whether that user is affiliated with a known research institution. While this won't be possible for all researchers, most legitimate researchers are affiliated with known research institutions, and so validation further reduces the overall research integrity risk and provides a pathway to hold offenders accountable. There are a variety of ways to do this, ranging from relatively simple techniques (is the user coming from a registered organizational IP address? Matching an email domain to known institutional domains) to more technically sophisticated (federated authentication). It's also possible to do this through traditional (but not scalable) methods, such as asking for confirmation from trusted colleagues.

Assess publication history: Legitimate researchers have a vested interest in growing a solid publication history, typically built over many years, because research is time consuming. In contrast, fraudulent identities tend to have either no prior history (they are created in bulk on demand) or an unrealistically large publication history (illegal enterprises have a commercial imperative to make as much use as possible of identities they're able to embed within editorial platforms). At scale, this can be addressed using trust markers, such as asserting an organizational affiliation in a researcher's ORCID record, or more sophisticated techniques like developing knowledge graphs.

It's important to recognize that any verification approach needs to offer multiple routes to trust. Early-career, unaffiliated, and technically limited researchers must have equivalent routes to verification, or we risk replacing an integrity problem with an exclusion problem.

You Can Help

STM's Researcher Identity group continues to develop these ideas and is now working to turn our framework into practical recommendations to help editorial platforms incrementally improve research verification over time. Working together, even small additional verification steps can help to make the cost of maintaining fraudulent identities too expensive for illegal enterprises and significantly reduce the flow of fraudulent submissions.

Ensuring that these changes don't disadvantage legitimate researchers is a challenge that the framework explores in some depth, but requires broader community engagement. If you have ideas or feedback on our recommendations, or want to share your perspectives on researcher verification, please use this form. We welcome your input.

Tim Lloyd

Tim Lloyd is founder and CEO of LibLynx, a company providing Identity, Access & Analytics solutions for online resources. His career spans several decades in a variety of product development and operational roles in online publishing, with a particular focus on developing innovative products and services to support online learning and research. Tim is a member of the Governance committee of SeamlessAccess.org and co-chair of the Outreach committee, a member of STM's Researcher Identity working group, and volunteers regularly to support a variety of industry initiatives.