Tech Policy Primer

Smart Reporting Channel for Federal Trade Commission Informants

Arjun Hassard
Justino Mora
Julia Uhr
Ritvik Vasudevan

To learn more about this project, please visit **aspentechpolicyhub.org.**

aspen institute

Smart Reporting Channel for Federal Trade Commission Informants

A guidance-first, privacy-preserving tool for reporting antitrust violations

EXECUTIVE SUMMARY

The Federal Trade Commission (FTC) should develop a smart user experience – including a secure communication channel – to improve the processing of antitrust violation reports, which are currently submitted by email. A structured submission workflow would assist prospective informants in figuring out the violation, and would also increase the usability of the report. With the ability to sort and label reports, FTC case teams would be able to more effectively filter, query, process, and authenticate submissions.

The underlying architecture of the entire smart user system, including that which facilitates communication between FTC staff and informants, should be transparent and open source. This would mean that informants would not be forced to simply trust that the security measures and privacy design of the system are sufficient; instead, independent organizations could provide oversight and catch vulnerabilities or design flaws.

BACKGROUND

Currently, the FTC uses a single email address to process all informant reports, irrespective of the antitrust violation being claimed (e.g., price fixing, refusal to deal, etc.). This approach's flaws include:

1 **Inefficiency**. Because the FTC provides an email address and not a set of form fields, submissions are entirely unstructured and vary from email to email. Case teams cannot perform basic queries to organize inbound reports, and emails may be missing critical information.

2 **Insufficient support for the informant and their attorneys.** On the FTC website, informants are given a few links to existing antitrust responses, and then they are asked to email their reports by answering a few simple questions. This "user journey" lacks important guidance. Although educational resources on antitrust violation categories do exist on the FTC's website, they are difficult to parse, far removed from the submission website, and not interactive, meaning many informants might miss them entirely.

3 **Privacy risks.** The FTC's current use of unencrypted emails adds risk of informants' identities being exposed, accidentally or otherwise. The onus is on the informant to protect their anonymity when submitting via this method, but they are provided with little help.

4 **Inhibited usage.** This lack of clarity on process, as well as the lack of support for informants on the current FTC website, may explain low submission volume. Perhaps not coincidentally, the Director of the FTC's Bureau of Competition in 2018 mentioned having difficulty 'finding antitrust cases.'

This approach is inadequate for several reasons. First, it falls behind global standards for informant reporting, including those of other federal agencies.

Second, if pending legislation passes, an email address may no longer be sufficient regardless. The FTC Whistleblower Act (FTCWA HR 6093) would reward and protect disclosures relating to suspected corporate violations of FTC regulations. If this legislation becomes law, we believe the FTC will need to better protect informant identities using technology, as greater financial incentives are likely to increase the risks undertaken by informants. These incentives are also likely to increase overall volume of reports, which makes improvements to informant support and violation categorization even more essential.

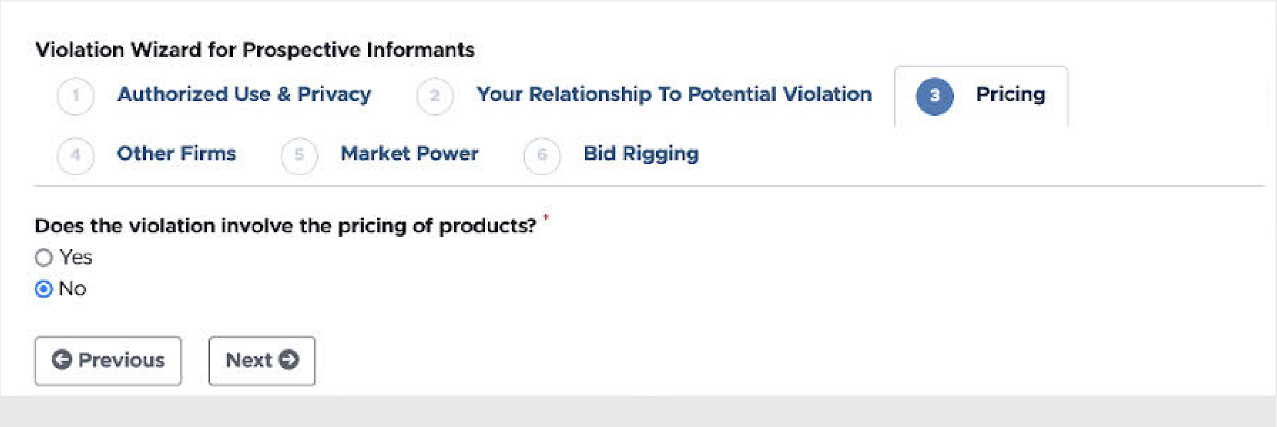
Finally, our proposal is not dependent on future laws — even if today the FTC cannot explicitly solicit reports from *whistleblowers*, it also cannot prevent *informants* from volunteering information about possible antitrust violations. **Improving security, privacy, and informant support in the reporting process is overdue.**

RECOMMENDATIONS

Smart Workflow UX

To improve the informant reporting system, the FTC should design and develop a new UX feature: a "smart workflow." Screenshots from a working prototype are below, and a video walkthrough is viewable here. In this example, the informant follows an adaptive wizard designed to identify the type of violation (in this case, the most likely category is *Bid Rigging*). In the screenshots below, the informant has already clicked through steps 1 and 2, which include a privacy statement and reporting the informant's relationship to the company in question.

i

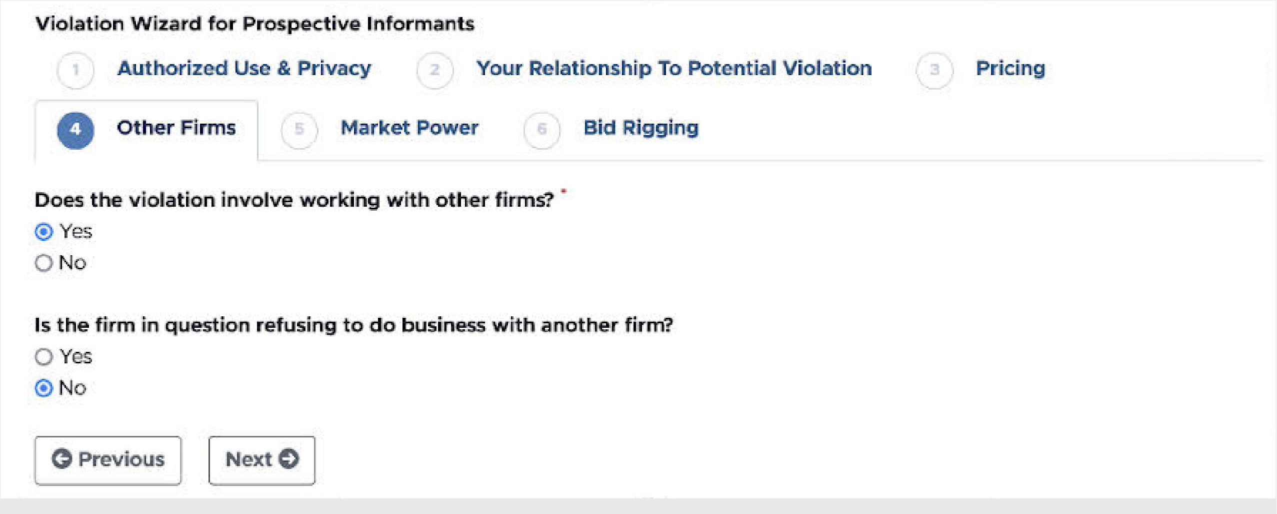

1 Authorized Use & Privacy
2 Your Relationship To Potential Violation
3 Pricing
4 Other Firms
5 Market Power
6 Bid Rigging
Previous
Next

Violation Wizard for Prospective Informants

Does the violation involve the pricing of products? *

○ Yes
● No

ii


1 Authorized Use & Privacy
2 Your Relationship To Potential Violation
3 Pricing
4 Other Firms
5 Market Power
6 Bid Rigging
Previous
Next

Violation Wizard for Prospective Informants

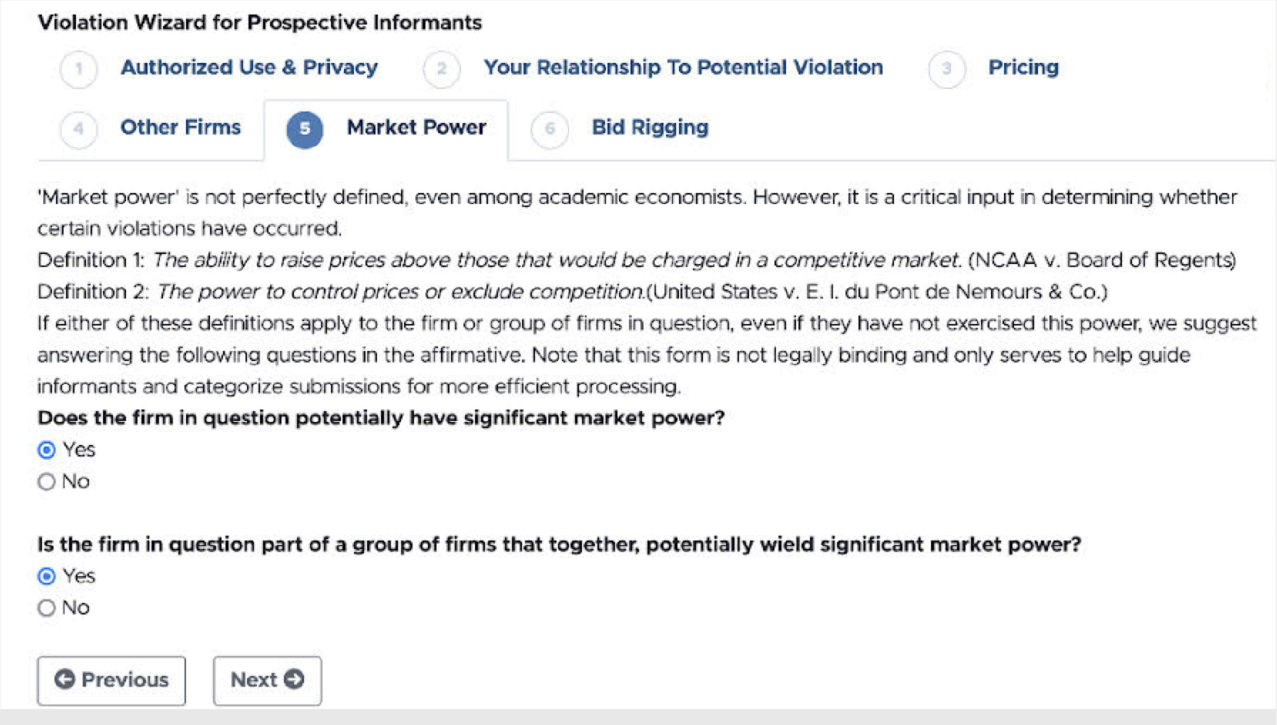
Does the violation involve working with other firms? *

● Yes
○ No

Is the firm in question refusing to do business with another firm?

○ Yes
● No

iii


1 Authorized Use & Privacy
2 Your Relationship To Potential Violation
3 Pricing
4 Other Firms
5 Market Power
6 Bid Rigging
Previous
Next

Violation Wizard for Prospective Informants

'Market power' is not perfectly defined, even among academic economists. However, it is a critical input in determining whether certain violations have occurred.

Definition 1: *The ability to raise prices above those that would be charged in a competitive market.* (NCAA v. Board of Regents)

Definition 2: *The power to control prices or exclude competition.*(United States v. E. I. du Pont de Nemours & Co.)

If either of these definitions apply to the firm or group of firms in question, even if they have not exercised this power, we suggest answering the following questions in the affirmative. Note that this form is not legally binding and only serves to help guide informants and categorize submissions for more efficient processing.

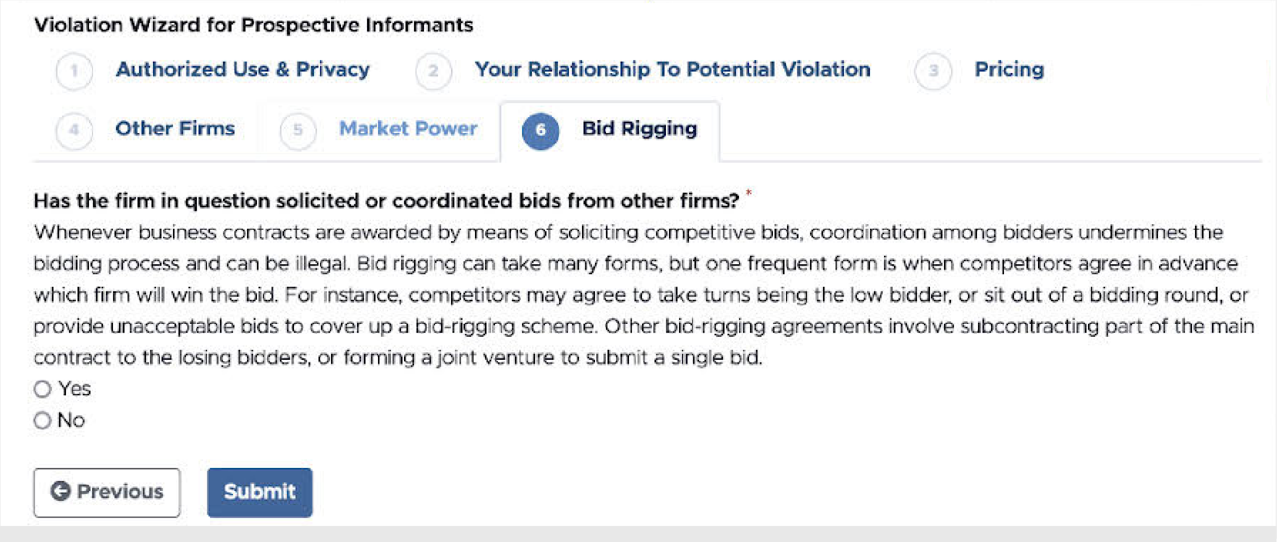
Does the firm in question potentially have significant market power?

● Yes
○ No

Is the firm in question part of a group of firms that together, potentially wield significant market power?

● Yes
○ No

iv


1 Authorized Use & Privacy
2 Your Relationship To Potential Violation
3 Pricing
4 Other Firms
5 Market Power
6 Bid Rigging
Previous
Submit

Violation Wizard for Prospective Informants

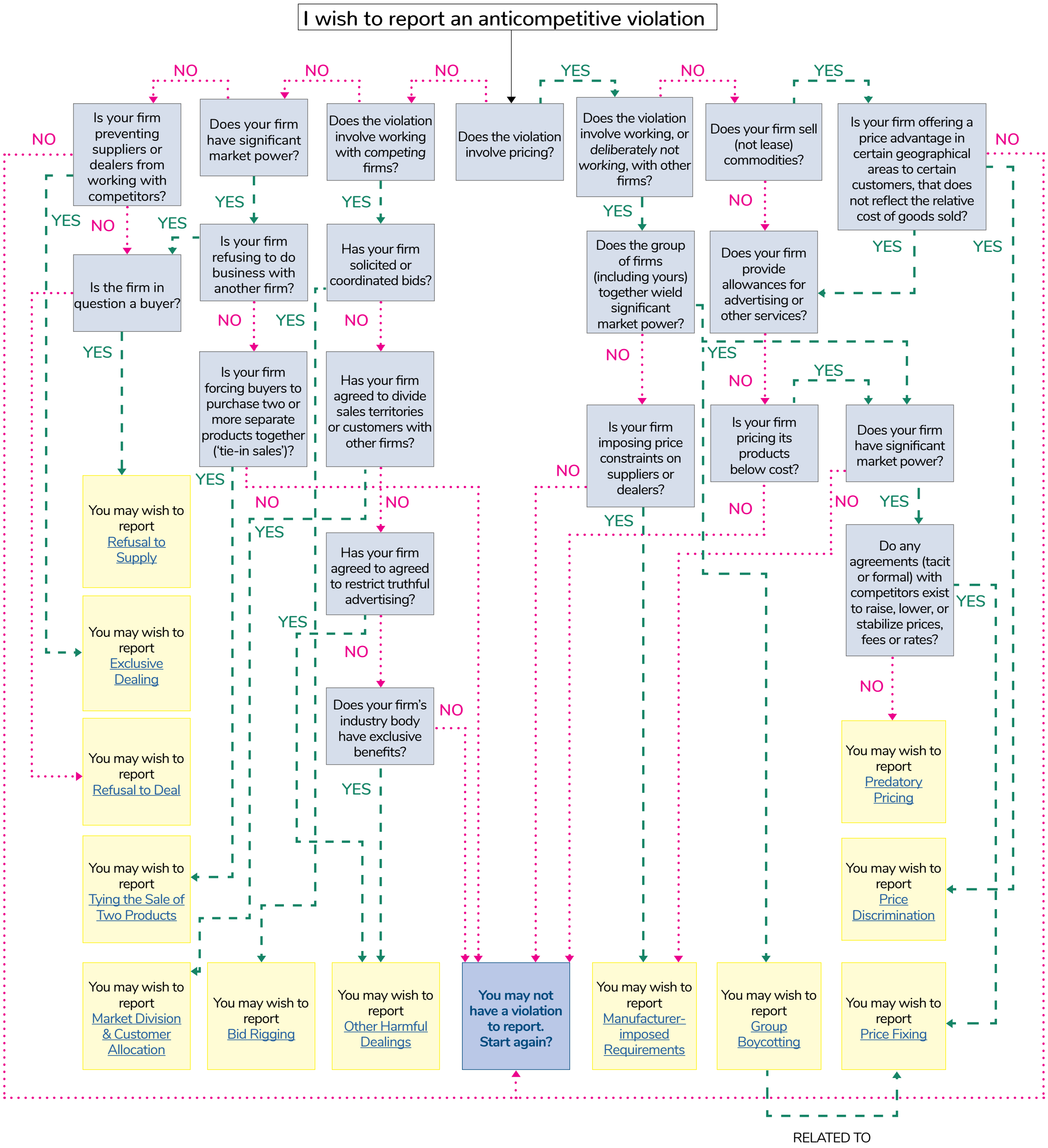
Has the firm in question solicited or coordinated bids from other firms? *

Whenever business contracts are awarded by means of soliciting competitive bids, coordination among bidders undermines the bidding process and can be illegal. Bid rigging can take many forms, but one frequent form is when competitors agree in advance which firm will win the bid. For instance, competitors may agree to take turns being the low bidder, or sit out of a bidding round, or provide unacceptable bids to cover up a bid-rigging scheme. Other bid-rigging agreements involve subcontracting part of the main contract to the losing bidders, or forming a joint venture to submit a single bid.

○ Yes
○ No

Screenshots of example user journey of the smart workflow tool.

A more comprehensive smart workflow is below, and is available for download and closer review here. This simplified diagram contains 12 possible violation endpoints, indicated by yellow squares.


I wish to report an anticompetitive violation
NO
NO
NO
YES
NO
YES
NO
NO
Is your firm preventing suppliers or dealers from working with competitors?
Does your firm have significant market power?
Does the violation involve working with competing firms?
Does the violation involve pricing?
Does the violation involve working, or deliberately not working, with other firms?
Does your firm sell (not lease) commodities?
Is your firm offering a price advantage in certain geographical areas to certain customers, that does not reflect the relative cost of goods sold?
YES
NO
YES
YES
YES
YES
NO
YES
YES
Is the firm in question a buyer?
Is your firm refusing to do business with another firm?
Has your firm solicited or coordinated bids?
Does the group of firms (including yours) together wield significant market power?
Does your firm provide allowances for advertising or other services?
NO
YES
NO
YES
NO
YES
NO
YES
Is your firm forcing buyers to purchase two or more separate products together ('tie-in sales')?
Has your firm agreed to divide sales territories or customers with other firms?
Is your firm imposing price constraints on suppliers or dealers?
Is your firm pricing its products below cost?
Does your firm have significant market power?
YES
NO
NO
NO
YES
NO
NO
YES
YES
You may wish to report Refusal to Supply
Has your firm agreed to agreed to restrict truthful advertising?
Do any agreements (tacit or formal) with competitors exist to raise, lower, or stabilize prices, fees or rates?
YES
YES
NO
NO
You may wish to report Exclusive Dealing
Does your firm's industry body have exclusive benefits?
NO
YES
You may wish to report Refusal to Deal
You may wish to report Predatory Pricing
You may wish to report Tying the Sale of Two Products
You may wish to report Price Discrimination
You may wish to report Market Division & Customer Allocation
You may wish to report Bid Rigging
You may wish to report Other Harmful Dealings
You may not have a violation to report. Start again?
You may wish to report Manufacturer-imposed Requirements
You may wish to report Group Boycotting
You may wish to report Price Fixing
RELATED TO

By requesting specific inputs from the informant and provisionally categorizing the violation, this smart workflow would:

1. Educate informants on what constitutes an antitrust violation, while simultaneously narrowing down the category of each violation;
2. Help informants gather the strongest evidence to support investigation;
3. Maximize the usability of the report(s);
4. Help informants make a well-informed decision before engaging with the agency;
5. Save FTC case teams significant time spent on filtering, segmenting, and evaluating reports;
6. Reduce the number of irrelevant and inadmissible reports;
7. Enable automated routing of reports to reviewers with specific domain expertise; and
8. Enable direct querying submissions without any data preparation, manual review, or machine learning.

Provably Secure System

The FTC should also build and deploy a new smart informant channel using transparent and open source software. This would enable civil society members, including specialist NGOs, privacy advocacy groups, and other technical contributors, to audit the system and uncover any vulnerabilities, back-doors, or other flaws. **This system would provide superior assurances to prospective informants that their identity – as well as the sensitive information they supply – will remain secure and will be shared only with explicitly designated recipients (e.g., FTC case teams)**. Informants would not be forced to simply trust the software vendor that runs the system on behalf of the agency. Moreover, such a system would also insure the FTC against (a) cyberattacks that seek to deanonymize informants and (b) accidental leaks of sensitive information.

Evidence suggests that these security protocols would help improve the quality of FTC submissions. A 2021 study conducted by EQS Group and the University of Applied Sciences of the Grisons found that organizations with **specialized reporting channels, such as a secure digital channel, were more likely to receive relevant whistleblowing reports** than organizations with more basic ways of filing, such as via an email address. Similarly, the US Securities and Exchange Commission (SEC), which has invested greatly in improving its informant/whistleblower programs in the past decade, also endorses (a) improving reporting systems by providing informants with educational resources, (b) greater system transparency, and (c) better processing efficiency on the agency side.

OPERATIONALIZATION

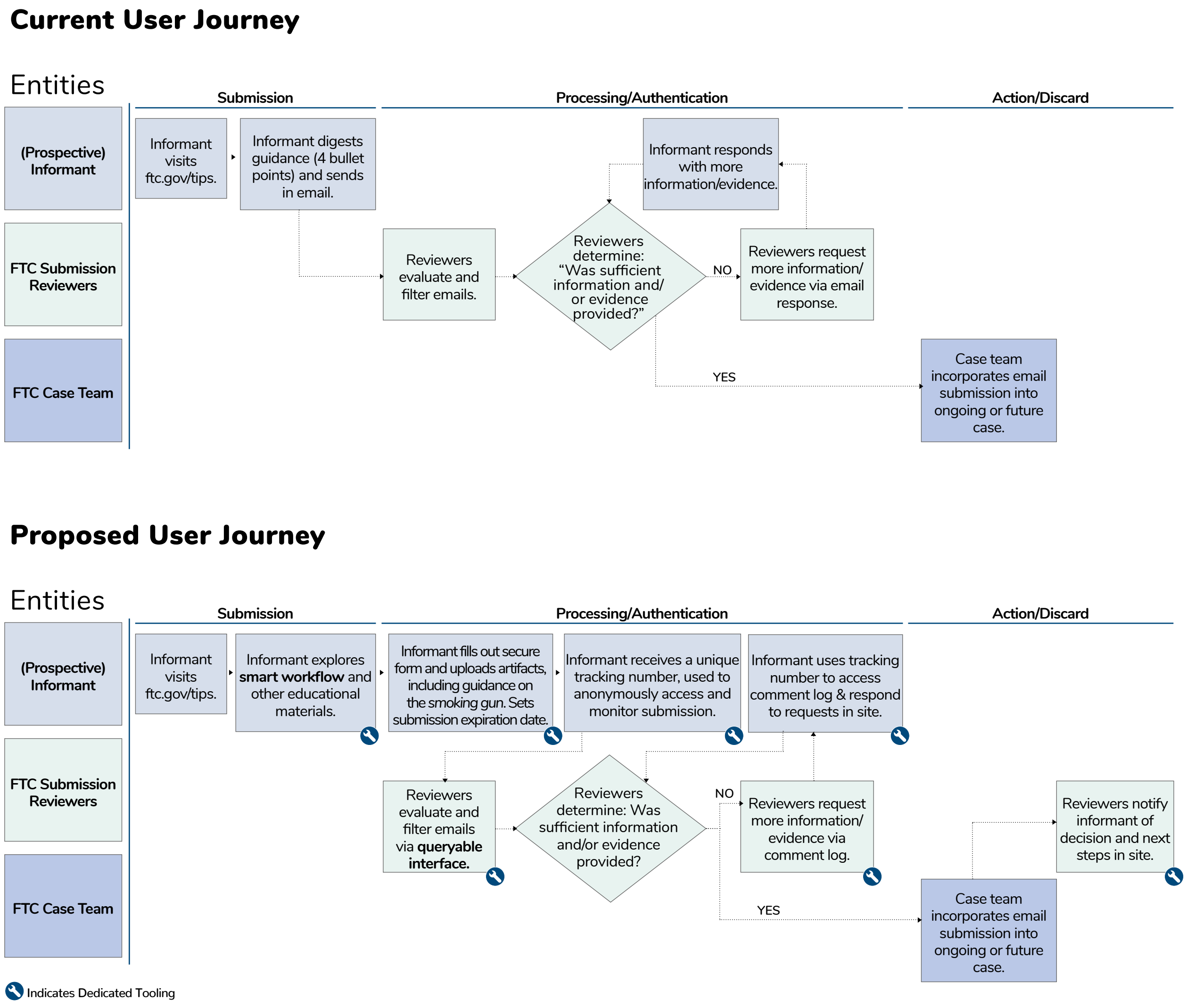
There are several (not mutually exclusive) ways the FTC might pursue these recommendations. They include building a variation of the SEC's tip form and deploying a free and open source software framework such as GlobaLeaks. The current working prototype is built using GlobalLeaks.

Solution	Pros	Cons	Cost Estimates
Build a variation of the SEC's existing Tip Form.	‣ The SEC's form leverages state-of-the-art materials from an existing agency partner. ‣ It provides more structure and guidance for report submissions than an email address. ‣ The SEC can share code for the Tip Form with the FTC as part of the Federal Source Code Policy.	‣ The Tip Form is tailored to financial crimes, not antitrust violations. ‣ It could introduce operational complexity given that the SEC already relays tips to the FTC. ‣ Forking the FTC's work makes it difficult for them to benefit from SEC-led enhancements. ‣ The system will still require development and maintenance to be compatible with the FTC's backend systems.	‣ Between 100–150 FTE person-hours.

Solution	Pros	Cons	Cost Estimates
Build the UX and channel with the GlobaLeaks framework, or another free and open source software.	- The security and architecture of GlobaLeaks are publicly auditable, and it is already utilized by various public institutions, particularly in Europe. - GlobaLeaks leverages prior work by offering relevant built-in features, such as anonymity-preserving communication between informants and case teams. - The technical requirements for launching an instance of GlobaLeaks are minimal. - GlobaLeaks offers many customizable templates for user flows, which are sophisticated enough to accommodate the smart workflow included in this proposal.	- Adopting open source technology may meet cultural resistance. - Such technology may require a security evaluation by an established auditor of government agency technology. - While GlobaLeaks provides a high level of out-of-the-box customization, there may be UX requirements that necessitate front-end development work. - The system will require some development and maintenance to be compatible with the FTC's backend systems.	- The costs for running a robust, highly available, and secure version of Globaleaks for 1 year is estimated to be **$2,800** and between **232-256** FTE person-hours.

Proposed User Journey (versus Status Quo)

Our proposal interface would add steps to the report submission process that are critical to guide and narrow inbound reports. Please see the below user journey for more information on the user experience.



Current User Journey

Entities
Submission
Processing/Authentication
Action/Discard
(Prospective) Informant
FTC Submission Reviewers
FTC Case Team
Informant visits ftc.gov/tips.
Informant digests guidance (4 bullet points) and sends in email.
Informant responds with more information/evidence.
Reviewers evaluate and filter emails.
Reviewers determine: "Was sufficient information and/or evidence provided?"
NO
Reviewers request more information/ evidence via email response.
YES
Case team incorporates email submission into ongoing or future case.

Proposed User Journey

Entities
Submission
Processing/Authentication
Action/Discard
(Prospective) Informant
FTC Submission Reviewers
FTC Case Team
Informant visits ftc.gov/tips.
Informant explores smart workflow and other educational materials.
Informant fills out secure form and uploads artifacts, including guidance on the smoking gun. Sets submission expiration date.
Informant receives a unique tracking number, used to anonymously access and monitor submission.
Informant uses tracking number to access comment log & respond to requests in site.
Reviewers evaluate and filter emails via queryable interface.
Reviewers determine: Was sufficient information and/or evidence provided?
NO
Reviewers request more information/ evidence via comment log.
YES
Case team incorporates email submission into ongoing or future case.
Reviewers notify informant of decision and next steps in site.
Indicates Dedicated Tooling

Current and Proposed User Journey

Overall Staffing and Costs

If the FTC were to adopt GlobaLeaks, the total budget for this program for one year is estimated to be $2,800 in technology costs and between 232–256 FTE person-hours. As such:

- We suggest that 2 full-time employees work on the initial setup and configuration of GlobaLeaks to ensure it is built with scalability, high availability, performance, and security in mind. The first 2 weeks of staff time should be focused on launching a working version of GlobaLeaks on the FTC's desired cloud service provider.
- Assuming the FTC uses a standard cloud service provider such as Amazon Web Services (AWS), the FTC should expect to spend about $2,800 on cloud services in the first year, as calculated using AWS's $233/month; see associated budget estimate).
- Maintenance and development costs would consist of 6–8 staff-hours per month to further customize and update GlobaLeaks when new versions and security patches are released.

Tech Policy Primer

ABOUT THE TECH POLICY PRIMER

This project was completed as part of the Aspen Tech Policy Hub's Tech Policy Primer program, a 10-week, part-time program that trains science and technology experts on the policy process. Learn more at **aspentechpolicyhub.org/primer.**

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

aspen institute