CHARITY & SECURITY NETWORK

Issue Brief

August 2019

Financial Services Deplatforming Hurts Aid, Peacebuilding

Increasingly, financial service companies and online payment platforms are bowing to pressure from outside groups to "deplatform" or cancel the accounts of nonprofit organizations (NPOs) and human rights defenders working in global hot spots. This affects humanitarian aid, peacebuilding, development and human rights programs. Organizations with a self-professed political agenda are manufacturing and using disinformation to pressure financial service companies and payment platforms to end their relationships with these NPOs. Ostensibly, these ideologically motivated groups claim their actions are aimed at strengthening security, but they are in fact contributing to insecurity by impeding the NPOs' legitimate work.

In an example of this troubling trend, organizations that are hostile to Palestinian rights are manufacturing and using disinformation to pressure financial service companies and payment platforms to end their relationships with NPOs working in the Occupied Palestinian Territory (OPT), or with Palestinians, in an effort to disrupt the NPOs' assistance efforts. They seek to put political pressure on Palestinians by denying them basic assistance. Many openly boast of their anti-Palestinian rights agenda.

These groups erroneously tell the platforms that the NPO is associated with, working with or funding a listed terrorist group, and raise the spectre, usually in forceful yet unsubstantiated terms, that keeping these accounts open puts the company at legal risk. Because the disinformation used in these deplatforming campaigns alleges ties to organizations that might be involved in furthering or supporting terrorist acts, the online platforms are understandably concerned about prosecution for material support, sanctions violations and/or reputational damage. However, targeted NPOs are generally legitimate organizations recognized by regulatory authorities that, unlike white supremacy groups that promote violence, provide essential services and at times engage in constitutionally protected speech. These deplatforming campaigns are exploiting legitimate concerns about accountability and legality, and the platforms are being used as a tool for a political agenda.

These attacks are part of a broader coordinated campaign that includes the publication of false, slanderous or misleading information; targeted lobbying and proposed legislation; delegitimization; and baseless legal actions. These tactics, targeted at groups with which they disagree, aim to delegitimize and silence lawful, legitimate and often lifesaving nonprofit work. Disinformation about NPOs that work in conflict zones, with politically marginalized communities, or that speak out against human rights abuses is nothing new, as seen on websites, blogs and social media platforms.[1] Groups spreading this disinformation have now taken their messages to the financial services industry.

[1] See, e.g., Carlos H. Conde, "Philippines Disinformation Campaign in Geneva," Human Rights Watch, July 6, 2019, https://www.hrw.org/news/2019/07/06/philippines-disinformation-campaign-geneva and Paul M. Barrett, "The Disinformation Problem Starts at Home," Wired, March 14, 2019, https://www.wired.com/story/disinformation-domestic-problem/

Unfortunately, the lack of clear, transparent policies at financial service firms means that all of their clients are vulnerable to politically motivated campaigns. Decisions to deplatform may be made on an ad hoc basis, and the NPOs that lose their accounts have no means by which to set the record straight. Companies should take steps to prevent their platforms from being abused by politically motivated agendas.

Harmful Impacts

The inability to collect and process online donations can have devastating consequences for NPOs' ability to provide vital services to the world's most vulnerable populations. In the banking sector, examples have come to light of lifesaving assistance stymied as a result of charities' inability to transfer funds to foreign countries, including humanitarian disasters in Syria, Somalia and other conflict areas. This constitutes a serious and systemic challenge for the continued delivery of vital humanitarian and development assistance – part of core human values.

Payment platforms are extremely centralized. Because payment service providers like MasterCard and Visa are so large and bind smaller entities like PayPal, Stripe, and many of the Bitcoin payment services, they are able to act as gatekeepers.[2] So while many argue that consumers can choose which companies to do patronize and the companies can choose their customers, that does not hold true with payment providers. Although these companies operate as private enterprises, they have essentially taken on the role of government censor. When an NPO is the customer, there is an outsize impact.

Robust Regulation and Due Diligence of NPOs

There has for some time been a perception in the financial services community that NPOs are easy conduits for terrorist financing. This is based on outdated thinking that has since been debunked by multilateral standard-setting bodies as well as the U.S. Treasury.[3] The high level of transparency, regulatory oversight and good governance of U.S. NPOs in particular has made it extremely difficult for terrorist financiers to use legitimate NPOs as a source of funding.

NPOs are subject to a variety of reporting and public disclosure requirements. In the U.S., for example, federal regulation requires compliance with extensive requirements to ensure activities and spending are exclusively for tax-exempt (charitable) purposes. State charity regulators oversee incorporation and governance of nonprofits, and, along with many municipalities, regulate fundraising to prevent fraud. Furthermore, NPOs undertake voluntary audits and participate in good governance programs. NPOs that work in global hot spots where aid is desperately needed take the threat of diversion of assets to terrorism very seriously. Because of their extensive field experience, they know first-hand the dangers of working in proximity to terrorist-listed armed groups. In addition to protecting against physical attacks, NPOs also employ extensive due diligence procedures to ensure that their financial resources are used solely for charitable purposes.

---

[2] Rainey Reitman, "The Kafkaesque Battle of Soulseek and PayPal , and Why Free Speech Defenders Should Be Worried About Payment Networks," Electronic Frontier Foundation, Feb. 25, 2016, https://www.eff.org/deeplinks/2016/02/kafkaesque-battle-soulseek-and-paypal-and-why-free-speech-defenders-should-be

[3] See U.S. Dept. of Treasury, *National Terrorist Financing Risk Assessment* 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf; Financial Action Task Force, Recommendation 8 on Nonprofit Organizations, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 11

In the rare cases where terrorist financing is tied to charities, it is usually terrorist fronts, or sham charities, created by criminals and terrorists, that are involved.[4] Because the main line of defense against these types of groups is government oversight and regulation, it is relatively easy for financial service providers to distinguish sham from legitimate charities.[5]

Customer Rights and Remedies

Because there is no comprehensive federal or state consumer protection law regulating non-banks, such as PayPal,[6] Stripe and others, the rules are dictated by the online financial services providers themselves, in their Terms of Service (TOS). These generally provide the provider with the right of termination at any time for any reason.[7] Similarly, crowdsourcing platforms not only include these types of termination clauses, but also incorporate the TOS of the payment processors with whom they work.[8] Some companies may cite their TOS when choosing not to do business with "problematic" clients at the outset (rather than deplatforming them later).

These TOS are far from robust in terms of clarity or customer protection. Payment processor Stripe has a Restricted Businesses policy that prohibits, among other things, any business or organization that "engages in, encourages, promotes or celebrates unlawful violence or physical harm to persons or property."[9] These policies can be easily exploited by those with political agendas peddling false information about NPOs.

Additionally, there is no recourse for a NPO client that has been deplatformed due to a politically motivated disinformation campaign, and there is no transparency around how platforms' decide which clients to drop. As the changetheterms.org campaign notes, "Most tech companies are committed to providing a safe and welcoming space for all users, even if they have so far failed to follow through on that commitment. But when tech companies try to regulate content arbitrarily, without civil rights expertise, or without sufficient resources, they can exacerbate the problem."[10]

---

[4] Data from the Department of Treasury's 2018 National Terrorist Financing Risk Assessment supports this conclusion. U.S. Dept. of Treasury, *National Terrorist Financing Risk Assessment* 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf at 24.

[5] Sham charities, for example, are unlikely to fill out the annual IRS filing known as the Form 990, publicly available via the database at Guidestar.org.

[6] See Mark E. Budnitz, *The Legal Framework of Mobile Payments*, Pew Trusts, Feb. 10, 2016, www.pewtrusts.org/~/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf

[7] For example, Payroc's TOS states, "We may terminate these Terms of Service or any Additional Terms, or suspend or terminate your iTransact Account or your access to any Service, at any time for any reason. We will take reasonable steps to notify you of termination by email or at the next time you attempt to access your iTransact Account. You may also terminate the Terms of Service and Additional Terms applicable to your iTransact Account by deactivating your iTransact Account at any time." http://itransact.com/downloads/itransact_user_agreement.pdf

[8] DonorBox's TOS, for example, incorporates those of PayPal and Stripe, https://donorbox.org/terms. In addition, the TOS provides "No Liability for Termination." https://donorbox.org/terms. Similar TOS provisions can be found at https://democracyengine.com/terms-of-service/; https://stripe.com/en-US/ssa; and www.paypal.com/us/webapps/mpp/ua/useragreement-full

[9] Stripe, Restricted Business, Last Updated March 15, 2019, https://stripe.com/en-US/restricted-businesses

[10] Changetheterms.org is a coalition of 40 civil and human rights organizations with the goal of providing "greater structure, transparency, and accountability" and fair policies that are effectively enforced by tech companies. Their model terms of service and other documents reflect the goals of a related campaign widely known as 'Deplatform Hate.' While the Twitter handle @deplatforminghate, which has led to the deplatforming of right wing groups, appears to be owned by an anonymous individual, the campaign organized by Color of Change can be found at www.bloodmoney.org. It seeks to "remove the services [of financial platforms] from dozens of hate sites, and to create internal policies to stop profiting from bigotry." We recognize that this campaign raises important and difficult free speech issues, and support the ultimate goal of curtailing the activities of violent hate groups. However, we do not take a formal position on that campaign's tactics. We do, however, find some aspects of changetheterms.org's model terms of service and recommended corporate policies useful.

Recommendations for Financial Platforms and other Service Providers[11]

In the absence of regulations governing online payment platforms, there is a need to establish transparency and consistency around how companies decide to deplatform, as well as a fair and open process to appeal decisions. Some recommendations follow:

1. Establish cooperation between the platforms and NPO advocacy or umbrella groups that represent charities that have been targeted by politically motivated disinformation campaigns.
2. Educate platforms on disinformation and defamation. Develop clear, objective criteria to identify groups using disinformation so that financial service providers do not fall prey to these campaigns.
3. Create a board, committee or team made up of persons with demonstrated expertise on matters pertaining to the company's terms of service (hate, free speech, disinformation, extremism, etc.) to establish policies and procedures for accepting and terminating clients, as well as to adjudicate appeals.
4. Create a fair and open right to appeal any material impairment, suspension, or termination of service. This should include the statement of a reason for the denial of service at the time of denial, with a clear explanation of the specific activities that led to the denial.
5. Provide a neutral decisionmaker with sufficient expertise in the matters pertaining to the denial to adjudicate the appeal.
6. Periodically test the company's policies and procedures to ensure that they are not biased against any persons or groups.

Conclusion

Financial services companies are bowing to pressure from groups with self-professed political agendas to cancel the accounts of humanitarian, development, peacebuilding and human rights groups working in global hot spots. While these groups claim that their efforts strengthen security or combat discrimination, they are actually creating and using disinformation to delegitimize and disrupt NPOs' legitimate and legal work to further their ideological strategy. Financial service providers should not allow their platforms to bolster and do the work for these interests. In falling prey to these organizations, they are impeding the work of groups aligned with core human values.

Transparent corporate terms of service that are formulated in consultation with persons who have demonstrated expertise on matters pertaining to the company's terms of service; clear, objective criteria; and a fair and open right to appeal will best serve the interests of both the financial service companies and their customers.

[11] Many of these are drawn or adapted from changetheterms.org. Their model TOS include provisions on enforcement; right of appeal; transparency; evaluation and training; governance and authority; and state actors, bots and trolls.

For more information contact:

Charity & Security Network
700 12th St. NW, Suite 700, Washington, DC 20005
info@charityandsecurity.org www.charityandsecurity.org @CharitySecurity