NSSF
The Firearm Industry Trade Association

LAWRENCE G. KEANE
SVP Gov't & Public Affairs, Assist. Secretary and General Counsel
lkeane@nssf.org | 202-220-1340 x 249 | nssf.org
400 N. Capitol Street NW, Suite 475, Washington, D.C. 20001

August 5, 2026

ATF Rulemaking Comments
Office of Regulatory Affairs
Enforcement Programs and Services
Bureau of Alcohol, Tobacco, Firearms and Explosives
99 New York Avenue NE, Mail Stop 6.N-518
Washington, DC 20226

RE: Comment on RIN 1140-AB05; Docket No. ATF-2026-0266; ATF No. 2025R-26P; Revising Non-Over-the-Counter Firearms Transaction Requirements

Dear Sir or Madam,

On behalf of the National Shooting Sports Foundation ("NSSF"), the Firearm Industry Trade Association, I am writing to submit comments regarding the above-referenced Notice of Proposed Rulemaking (the "NPRM"), which was published by the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") for comment on May 8, 2026.[1] This NPRM proposes amendments to 27 C.F.R. §§478.96 and 478.124, allowing for expanded "non-over-the-counter" ("NOTC") sales of firearms, specifically in regards to transactions that are subject to completion of a National Instant Criminal Background Check System ("NICS") and identify verification of the transferee.

The proposed amendments provide a process by which federal firearms licensees ("FFLs") may complete retail sales subject to a NICS check, without the purchaser presenting themselves in person at the licensee's premises. This process, in addition to the requirements of completing a Form 4473, and conducting a NICS check, requires licensees to verify the purchaser's identity through videoconferencing, and to obtain an independent verification of identity through the use of a credential service provider ("CSP"), along with additional requirements applicable to all NOTC transactions. Such transactions are currently not permitted under ATF regulations, which only contemplate NOTC transactions for NICS-exempt sales.

[1] FR Doc. 2026-09157

While NSSF agrees with ATF's interpretation that 18 U.S.C. §§922(c) and (t) do not prohibit NOTC transactions where a sale is subject to a NICS check, we write today to raise concerns on behalf of our members regarding the public safety implications of allowing such transactions.[2]

The Firearm Industry is on the Frontline in Preventing Illegal Purchasing of Firearms

As ATF itself has recognized, FFLs are the "first line in maintaining the security and lawful transfer of firearms."[3] This is a role and responsibility that the entire industry takes most seriously. Ensuring prohibited persons, straw purchasers, and illegal firearm traffickers do not gain access to firearms is critical to preventing crime and keeping our communities safe.

To these ends, NSSF, as the Firearm Industry Trade Association, has initiated and operates numerous programs aimed at raising awareness of firearm safety and security, educate retailers on identifying red flags for potentially illegal purchases, promote the responsible use and storage of firearms by purchasers, and encourage interventions with those at risk of self-harm. Many of these programs are joint initiatives between NSSF and ATF. NSSF's initiatives include:[4]

- Project ChildSafe® - promoting responsible storage of firearms and providing free firearm locks in cooperation with law enforcement agencies and other partners;
- Operation Secure Store® - a joint initiative with ATF, providing retailers with actionable resources to improve the physical security of their locations, and prevent firearm theft;
- FixNICS® - an effort to encourage states and other government agencies to ensure that all disqualifying records are transmitted to the National Instant Criminal Background Check System;
- Have a Brave Conversation™ – an effort undertaken with the assistance of the American Foundation for Suicide Prevention to help concerned friends and family intervene with loved ones at risk of self-harm.

Most relevant to these comments, NSSF also partners with ATF on Don't Lie for the Other Guy™, a program aimed at educating the public about the penalties associated with facilitating a straw purchase, and providing resources to FFLs to train their employees on detecting straw

[2] NSSF would note that we are not taking the position with this comment letter that other NOTC transfers, which have been safely conducted by FFLs since the enactment of the GCA, including transfers to individuals with NICS-exemption qualifying permits, or transfers of National Firearms Act ("NFA") firearms, should be discontinued. Such transactions are subject to other additional verification procedures to ensure that transferees are not a risk for illegal diversion. For example, before a transfer of an NFA firearm can occur, ATF conducts an extensive background check on the transferee, and requires the transferee to submit photographs and fingerprints.

[3] ATF Publication 3317.2, Safety and Security Information for Federal Firearms Licensees (June 2021), https://www.atf.gov/media/22421/download.

[4] For more information on each of these programs, see https://nssfrealsolutions.org/.

purchases before they can occur.[5] Through this program retailers can obtain, for free, a kit with point-of-sale displays warning customers of the severe penalties for illegal firearms purchases, as well as important educational information on how to better recognize and avoid illegal purchases before they happen. These resources include training videos depicting common scenarios ATF has identified that retailers might encounter indicating an illegal purchase may be occurring.

Beyond providing these resources, NSSF and ATF also frequently collaborate to highlight the Don't Lie mission in targeted communities. These efforts bring together federal, state, and local law enforcement to reinforce the Don't Lie message, through targeted digital messaging, billboards, and audio public service announcements, reaching millions of individuals. The most recent of these campaigns was launched just last week in Indianapolis, and was announced by NSSF President and CEO Joe Bartozzi, along with ATF Special Agent in Charge Jorge Rosendo, U.S. Attorney Thomas E. Wheeler II, as well as numerous representatives from state and local law enforcement.

These initiatives all show the tremendous resources that the firearm industry has committed, and continues to commit, to ensuring that its products are not illegally purchased or diverted to the criminal market. As responsible corporate citizens, NSSF and its members are dedicated to taking those actions possible to prevent straw purchases, and the sale of firearms to prohibited persons or individuals who otherwise appear to present a risk of harm to themselves or others.

NSSF Membership is Overwhelmingly Opposed to the NPRM

Following the NPRM's publication, NSSF polled its membership to determine whether they support or oppose the proposed rule.

The results of this polling were overwhelming, with 72% of NSSF members opposed to the NPRM, including a majority (56%) strongly opposed.[6] There was also minimal indication that members would take advantage of the new transaction options the proposed rule provides, with only 26% affirmatively indicating that they would choose to conduct NOTC transactions if the rule was made final.

While NSSF is not aware of the individual motivations each of these members have in supporting or opposing the proposed rule, we did receive from members additional sentiments in response to our polling. Among these, one of the primary sentiments expressed was a concern that expanded NOTC transactions would be exploited by bad actors to conduct illegal

---

[5] *See* https://nssfrealsolutions.org/programs/dont-lie-for-the-other-guy/; *see also* https://www.atf.gov/firearms/tools-services-law-enforcement/atf-firearms-programs/dont-lie-other-guy.

[6] NSSF Internal Polling conducted July 2026. Respondents comprised 624 members, including 557 retailers, 7 distributors, and 60 manufacturers.

straw purchases, or would otherwise allow for the completion of sales a retailer would deny due to their own suspicion arising from interacting with and observing the purchaser in person.

The comments that follow expand upon the common concerns members expressed in relation to public safety impacts the proposed rule may have if adopted.

NOTC Transfers Will Not Allow FFLs to Evaluate Purchasers for Suspicious Behavior

As already mentioned, ATF has itself recognized that FFLs are on the "first line of defense" in preventing unlawful purchases of firearms by straw purchasers and prohibited persons, and play a critical role in evaluating customers that enter their premises for suspicious behavior or other indications that they are seeking a firearm for unlawful purposes.

These tell-tales run a wide gamut, from evaluating the state-of-mind of a purchaser (looking for indicators of intoxication, or other indications that the purchaser may be a harm to themselves or others), to looking for other indications that the purchaser is either willfully purchasing, or being coerced to purchase, firearms on behalf of another, prohibited person or firearms trafficker.

When the only interaction between an FFL and a purchaser is filtered through the lens of a computer videocall, indicators of suspicious activity are greatly reduced. Clear indicators of intoxication or drug use, such as the odor of intoxicating liquors, abnormal pupil size, tract marks, or other physical manifestations may be hidden, or not perceptible through a videocall platform.

Likewise, common indicators of straw purchasing activity are unlikely to come across through a videocall interaction. One of the key indicators ATF has indicated that licensees should rely upon when determining whether a particular transaction might be a straw purchase is whether the purchaser is accompanied by other individuals.[7] If they are, and these individuals appear to be directing the nature of the purchase, or the purported purchaser appears to be fearful of or deferential to the other individuals, an FFL may choose to not move forward with the sale, on suspicion that the purchase is actually being made on behalf of or at the direction of the others present. When the only contact between an FFL and purchaser is within the bounds of a webcam, individuals who are actually directing a sale, or are the intended recipient of the

---

[7] *See* ATF, "How to Spot a Straw Purchase," https://www.atf.gov/firearms/tools-services-law-enforcement/atf-firearms-programs/dont-lie-other-guy ("Warning signs may include:

- One person selects the firearm while another person pays
- A buyer who appears unfamiliar with the firearm
- A purchaser being directed or coached by someone else
- Reluctance to complete required background check paperwork

If something doesn't seem right, it may not be.").

firearm, may easily hide off screen, and a transaction that otherwise would have been prevented by the in-person observation and due diligence of an FFL will be allowed to move forward.

Even more concerning, the limitations of a videocall may allow coercive parties to hide from view, and force individuals to make straw purchases on their behalf. If an individual is not required to be present to make a purchase, a bad actor could take advantage of the NOTC process to confine a victim and force them to conduct a purchase, all while remaining hidden from view of the FFL.

NOTC Transfers Could be Subject to Exploitation Through Deepfake or Other Deceptive Acts

The NPRM recognizes that the primary hurdle that has prevented the performance of expanded NOTC sales is the identity verification requirement contained at 18 U.S.C. §922(t)(1)(D), implemented by the Brady Handgun Violence Prevention Act. When this requirement was enacted, we were in a different age. The internet was only just gaining popularity, and videocalls were largely unknown or unavailable. ATF rightfully notes that technological capabilities have grown in leaps and bounds since that time, and that technology now exists which could allow for remotely verifying a person's identity. While this is certainly true, the same advances in technology, especially the recent surge in artificial intelligence ("AI") applications, have created unique risks of subversion which undermine the ability of FFLs to ensure identity verification procedures are reliable.

One of the most concerning recent trends in technology is the rise of "deepfake" applications. These are AI-powered tools that allow a user to change their appearance on video in real time, or even wholly create a fake avatar that appears on screen and mimics the expressions and voice of a user. The most powerful of these tools are so effective as to be nigh impossible to detect without counter-technology that looks for digital clues indicating that it is a generated image.

The concerns posed by this technology are not theoretical. Deepfake technology, and other AI generated imagery are widely used today, with more than 8,000,000 instances of deepfakes being cited in one analysis.[8] Fraud attempts involving deepfakes spiked 3,000% in 2023 alone,[9] and only 0.1% of consumers in one study could accurately differentiate between real and deepfake imagery (and participants were 36% less likely to correctly identify a deepfake video

[8] Nathan House, *Deepfake Statistics [2026]: Growth, Fraud & Detection Data*, StationX (August 2026), https://app.stationx.net/articles/deepfake-statistics#business-impact.

[9] Mohammed Khalil, *Deepfake Statistics 2025: AI Fraud Data & Trends*, DeepStrike (July 28, 2026), https://deepstrike.io/blog/deepfake-statistics-2025.

as compared to a still image).[10] Further, the use of deepfakes for fraudulent activity in the context of a live videocall is not unprecedented. Arup Hong Kong was the victim of a deepfake scam, which deceived an employee into joining a videoconference with what appeared to be several known colleagues, including the company CFO.[11] However, each of these apparent participants were deepfake avatars, based on publicly available videos of the personnel. Based on the instructions the employee received during this call, he was duped into transferring over $25,000,000 to the fraudsters.

It is entirely plausible that an identity thief could obtain a victim's ID, use a deepfake filter or AI avatar that is modeled after the photo on the ID (or other photos of the victim) and impersonate that victim in an identity verification video conference with an FFL, and in the identity verification process with a CSP.

While the risk of deepfakes is a known issue to those in the field, ensuring the integrity of any digital security or verification system against wrongful actors is inherently a continuous cat-and-mouse game. While technology may exist to weed out certain deception tools, new malicious methods to circumvent these controls and CSPs will always be catching up to close the gaps exploited by bad actors.

Regardless, an FFL is unlikely to have the sophisticated deception-detecting software and tools necessary to uncover a concealed identity during their own verification process, which leads to even greater potential exploitation. For instance, if a bad actor obtains access to an individual's CSP authentication account, they can use a deepfake during a videoconference with the FFL and avoid the potentially greater detection risk of interacting directly with the CSP.

In such cases where a bad actor has obtained unauthorized access to an individual's CSP account, such extreme measures may not even be necessary to subvert the FFL identity verification step. For example, where someone has obtained access to a victim's CSP account, they could create a separate fake ID matching the details indicated in the CSP account, but with their own photograph for the purposes of the FFL identity verification. Potential inconsistencies or other indicators of this ID's validity (or lack thereof) are less likely to be picked up on by the FFL in these cases, where they are unable to physically hold and examine the ID for known tell-tales of forgery. Instead, an FFL will only be able to examine the document through a video screen, and in the form of a scanned copy provided by the purchaser.

---

[10] *iProov Study Reveals DeepFake Blindspot: Only 0.1% of People Can Accurately Detect AI-Generated Deepfakes*, iPROOV (February 12, 2025), https://www.iproov.com/press/study-reveals-deepfake-blindspot-detect-ai-generated-content.

[11] *The ARUP Deepfake Fraud A PRMIA Case Study*, Professional Risk Managers' International Association (2025), https://prmia.org/common/Uploaded%20files/eCyber/PRMIA%20Case%20study%20-%20ARUP.pdf.

Each of these risks represent real avenues that could be exploited by straw purchasers, firearm traffickers, and other prohibited persons to obtain firearms. Without the availability of NOTC transactions, these bad actors face exceptionally higher hurdles to making an illegal purchase, not the least of which is the requirement to come face-to-face with a licensed firearms dealer with training and awareness of the red flags that indicate an individual is attempting to obtain a firearm unlawfully.

Conclusion

NSSF and its members are invested in taking those actions at industry's disposal to try to eliminate illegal straw purchases, and other unlawful firearm purchases wherever they occur. Ensuring prohibited persons, illegal straw purchasers, illegal firearm traffickers, and those who are intoxicated, under the influence of controlled substances, or otherwise appear to be a risk to themselves or others do not gain access to firearms is critical to preventing crime and keeping our communities safe.

As already discussed, NSSF's longstanding joint initiative with ATF, Don't Lie for the Other Guy, is expressly dedicated to educating the public about the penalties involved in committing an illegal straw purchase, and to assist ATF in providing resources and training materials to FFLs on how to detect such purchases before they occur.[12] The sentiments expressed by our members highlighting the potential public safety risks presented by the proposed rule evidence just how seriously members of the firearm industry take these lessons, and their role in ensuring that firearms do not fall into the wrong hands.

For the reasons set forth above, NSSF respectfully opposes this proposed rule because it undermines the ability and role of retailers to serve, as ATF recognizes, as the "first line of defense" in trying to prevent firearms getting into the hands of those who try to illegally obtain firearms or cannot be trusted to use them in a responsible manner.

Sincerely,

Lawrence G. Keane

Lawrence G. Keane

---

[12] For more information, see NSSF's website regarding this initiative, https://nssfrealsolutions.org/programs/dont-lie-for-the-other-guy/.