TECHNET
THE VOICE OF THE INNOVATION ECONOMY

TechNet Northeast | Telephone 774.230.6685
One Beacon Street, Suite 16300, Boston, MA 021081
www.technet.org | @TechNetNE

February 2, 2022

The Honorable Delegate CT Wilson, Chair
House Finance Committee
House Office Building
Annapolis, MD 21401

RE: TechNet Opposition to HB 295

Dear Chair Wilson and members of the Committee:

I write on behalf of TechNet respectfully in opposition to SB 295 – *Online Marketplace Disclosure Requirements*.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than three and a half million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

While SB 295 purports to protect consumers from illegal, stolen, or counterfeit goods, the legislation would in effect hurt small businesses and individual sellers who sell online. It would do little to slow organized retail crime, create privacy risks, conflict with federal law, and hamper marketplaces' technological ability to identify and remove illegal goods.

The internet has provided Maryland small businesses with the opportunity to instantly and conveniently sell their products to consumers across the globe. This legislation would unfortunately hurt their ability to compete by creating an onerous, time-consuming process of verification that big-box retailers would not have to deal with. As small businesses struggle to maintain profits while continuing to provide essential products to consumers during the COVID-19 pandemic, now would be an especially awful time to place additional, unnecessary regulations on them.

SB 295 would force Marylanders to compromise private information in order to continue selling on online platforms. Those unwilling to divulge highly personal information would be forced to stop listing their products and lose essential revenue streams. Platforms that have empowered so many individuals and small businesses to bring their products to market would be forced by the state to become marketplaces for unscrupulous individuals to shop for Maryland residents' personal data.

The fact is, many of TechNet's members have been working with the proponents of this legislation for over a year to strike a balance that addresses retail crime without exposing

innocent people's data to the world, and that balance is reflected in US House Bill HR 5502. The federal language addresses many of the most harmful flaws in the bill before you today, which was rejected by every state in which it was introduced last year, with the notable exception of Wal-Mart's home state of Arkansas. It also has the crucial benefit of being a 50-state solution, as opposed to the patchwork that would be created by each state attempting to address this on their own.

HR 5502 includes stronger privacy protections for small businesses that sell online, especially those that operate from home. It still requires the disclosure of email and/or phone number, but allows that information to be disclosed after a purchase if finalized and keeps a marketplace's ability to utilize other means of direct electronic messaging such as buyer/seller communication tools to qualify as contact information vehicles. This is much different than the bill before you today which would require the information to be plastered over the internet for anyone to consume and abuse. Having their information posted on each listing exposes sellers to very valid concerns of fraud, threats, and harassment. This is important because it helps ensure the marketplace is up to date with any buyer/seller communication. If buyers are encouraged to contact the seller off-platform or outside the buyer contact tools, there is no record or tracking of any issues that may arise. Not to mention, it could jeopardize the safety of sellers. The public could easily learn, for example, the name and home address of a grandmother in La Plata who makes and sells hand-knitted face masks or of a father in Leonardtown who has gotten into woodworking and sells his creations online, thus compromising their privacy. The open display of such personal information this bill would require of entrepreneurial Maryland citizens with innovative products and residents monetizing their hobbies alike could potentially lead to dangerous situations. In a time when policymakers and companies are working to improve privacy protection for individuals, this legislation is swimming against the tide of that progress.

The timelines for which a seller would be required to provide online marketplaces the required information for verification is also significantly different. The agreed-to federal bill allows the seller to submit the information within 10 days of becoming a high volume seller as opposed to the unreasonable 24 hours in the bill today. Many small businesses selling online are shops of 1 or a few individuals, so more flexibility in the timelines before their livelihoods are forcibly shut down is a critical change needed and acknowledged in the consensus federal bill.

And lastly, the agreed-to federal bill offers greater flexibility in the types of government issued records that are required to be submitted to a marketplace for verification. The federal bill strikes the requirement for an individual to provide a government issued IDs to include a physical address (e.g., Passports do not contain physical addresses, and would discriminate against those who don't have a government ID). Instead, the consensus federal bill allows the option of a seller providing the marketplace with a government issued tax document.

These are just some of the substantive concerns we have but taken together, are significant differences that persist in this bill that are not included in the federal, agreed-to bill. These modifications would safeguard consumers while protecting innovation,

giving online marketplaces flexibility in how to stop bad actors. Equally important, the federal bill would not favor one business model over another.

It is in each online marketplace's interest to maintain trust with the consumers using their platforms. The selling of illegal and counterfeit products is a serious issue, and that is exactly why online marketplaces are heavily invested in technologies, personnel, and processes that identify bad actors and remove them from their platforms. These tools are constantly being improved to ensure that they target bad actors on their platforms. Unfortunately, passage of this law is too prescriptive and not future proof, hampering the ability for online marketplaces to innovate as technology and bad actors evolve. Instead, we recommend the Committee consider the actions of states like Illinois, Michigan, and Connecticut, which have all established organized retail crime task forces that marshal the resources of law enforcement and retailers to stop this issue at its source.

We thank you in advance for your consideration, and please do not hesitate to reach out with any questions.

Sincerely,

Christopher Gilrein
Executive Director, Massachusetts and the Northeast
TechNet
cgilrein@technet.org