## TESTIMONY OF DREW GREENBLATT PRESIDENT AND OWNER MARLIN STEEL WIRE PRODUCTS

## "ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: ARE OUR LAWS ADEQUATE FOR TODAY'S THREATS?" MAY 13, 2014

## **BEFORE THE**

## U.S. SENATE JUDICIARY COMMITTEE, SUBCOMMITTEE ON CRIME AND TERRORISM

Chairman Whitehouse, Ranking Member Graham and members of the Subcommittee on Crime and Terrorism, thank you for your focus on the critical challenge of trade secret theft and for the opportunity to testify today.

My name is Drew Greenblatt, and I am the President and owner of Marlin Steel Wire Products LLC (<a href="www.marlinwire.com">www.marlinwire.com</a>), based in Baltimore, Maryland. Marlin Steel Wire is a leading manufacturer of custom wire baskets, wire forms and precision sheet metal fabrication assemblies – all produced here in America for the aerospace, automotive, medical, and pharmaceutical industries in the United States and 36 other countries around the world. I am here because:

- Trade secrets are vital for manufacturers of all kinds not just big companies, but also small firms like mine;
- America's trade secrets laws and policies must keep pace with today's threats,
   which increasingly are interstate and international; and

 Manufacturers need your help to effectively and efficiently protect and enforce trade secrets and to secure strong commitments in our trade agreements.

Like so many other manufacturers, Marlin Steel Wire competes in a global economy. We succeed through investments in ideas and innovations and through the hard work of our dedicated employees. When I bought Marlin Steel Wire Products back in 1998, we were a local business making bagel baskets, with roughly \$800,000 in sales and 18 employees. Last year, we had almost \$5 million in sales. We now have 24 employees.

Marlin is a proud member of the National Association of Manufacturers (NAM) and the National Alliance for Jobs and Innovation (NAJI). The NAM (<a href="www.nam.org">www.nam.org</a>) is the largest industrial trade association in the United States, representing more than 12,000 manufacturers large and small in all 50 states. In fact, the average company that NAM represents has between 35 and 40 employees. I serve on the NAM's Board of Directors and its Executive Committee.

I am also the co-founder and chairman of NAJI (<a href="http://naji.org">http://naji.org</a>), an alliance of 35 business associations and some 380 manufacturers across the country. NAJI works to defend the critical innovative aspects of advanced manufacturing by preventing unfair competition resulting from foreign manufacturers exploiting pirated software and other stolen intellectual property. Both the NAM and NAJI are working hard to strengthen protection of trade secrets and other intellectual property in order to level the playing field for businesses in the United States.

Today, trade secrets are more important than ever to manufacturers small and large. These vital intangible assets include everything from proprietary manufacturing plans, software, processes and formulas to research, marketing data and customer lists. The trade secrets of publicly traded U.S. companies alone are worth an estimated \$5 trillion. The knowledge assets of private companies like mine surely add much more to the total.

Small businesses, in particular, rely on trade secrets to protect their innovations, often because they are less expensive to retain and enforce than patents. For Marlin Steel Wire, trade secrets <u>are</u> our intellectual property – our "secret sauce." We leverage the expertise of our employees – 20 percent of whom are mechanical engineers – to manufacture custom-designed products that meet specific customer performance requirements through proprietary processes.

That's why addressing the serious and growing threat of trade secrets theft is so essential. Trade secrets increasingly are at risk in today's mobile and interconnected global marketplace. Estimates of losses from trade secrets theft range from one to three percent of GDP in the United States and other advanced developed economies. The head of the National Security Agency and U.S. Cyber Command believes theft costs American companies \$250 billion per year.

In our parents' or grandparents' day, trade secrets often were stolen by individual employees acting alone. They took paper documents and sold them to competitors across town. Now, trade secrets are digital and vulnerable to viruses spread through nefarious websites and hackers operating as part of criminal enterprises. Proprietary information that might once have taken a moving truck to transport can walk out the door on a thumb drive and be sold to governments or competitors across the coutnry or half a world away.

Trade secret theft is increasingly international in scope. As documented in recent reports by the Office of the National Counterintelligence Executive<sup>3</sup> and the Defense Security Service,<sup>4</sup> foreign governments like China and Russia are working

<sup>&</sup>lt;sup>1</sup> Center for Responsible Enterprise and Trade and PWC, <u>"Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats,"</u> February 2014.

<sup>&</sup>lt;sup>2</sup> Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History," Foreign Policy, July 9, 2012.

<sup>&</sup>lt;sup>3</sup> Office of the National Counterintelligence Executive, <u>"Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,"</u> October 2011.

<sup>&</sup>lt;sup>4</sup> Defense Security Service, <u>"Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting,"</u> 2013.

systematically to access the trade secrets of businesses in the United States and many other countries. Through cyber incursions, they are targeting and stealing advanced manufacturing and other technologies.

Trade secrets are acquired and developed through many years of company experience and investment. They provide a powerful business advantage in highly competitive sectors like manufacturing – but only as long as they remain confidential. Trade secrets are not exclusive rights. Once disclosed, their value is lost forever. Theft has a real, measurable, real-world impact. It costs good-paying U.S. jobs and can even put entire businesses at risk.

Cyber incursions not only threaten proprietary information, but also our people and products. Today, the lasers, robots and other machinery that drive advanced manufacturing are all connected to networks. At Marlin Steel Wire, we are safety nuts. Our plant has worked 1,975+ days without a lost time accident. But if hackers interfere with our machinery, they can put the safety of our workers at risk and destroy production runs. We can't let that happen.

That's why we are doing everything we can to harden our networks and safeguard our trade secrets. At Marlin Steel Wire, we protect trade secrets through non-disclosure contracts and technological security measures. We educate our employees about the importance of protecting proprietary information and the potential business impact if trade secrets are stolen or disclosed. Those measures are costly, but unfortunately all too necessary. For the amount I spend on security, I could hire another full-time welder. There are a lot of unemployed welders in Baltimore.

But there is only so much Marlin Steel Wire and other companies can do alone. Congress and the Administration have critical roles to play in ensuring America's laws, policies and law enforcement actions are equal to today's threats. The good news is that Washington is recognizing the problem. Congress has introduced and passed

legislation that is helping to upgrade our nation's laws for the 21<sup>st</sup> century. The White House has organized federal agencies behind a strategy to mitigate trade secret theft.<sup>5</sup>

The FBI has increased criminal enforcement of trade secret theft, conducting more investigations. The Foreign and Economic Espionage Penalty Enforcement Act, passed by both houses of Congress and signed in to law last year, went a long way to putting deterrent penalties in place. But that's not enough. We need to step up our game. Congress and the Administration must prioritize three actions that can raise the stakes for criminals, hit thieves in their wallets and better enable businesses to protect and enforce their rights.

First, we need strong operational collaboration between federal agencies as well as more engagement between those agencies and the business community. Protecting and enforcing trade secrets can't be the job of just one agency – a silo approach to a broad problem. We need a comprehensive, integrated push. The FBI, Justice, Customs and other agencies must work together to increase investigations and prosecutions, track down illicit gains and deliver real-time information to businesses about cyber threats and how to respond.

Second, we need access to federal civil enforcement for trade secrets theft, which well-conceived legislation like the Defend Trade Secrets Act recently introduced by Senators Chris Coons (D-DE) and Orrin Hatch (R-UT) would provide. Despite their strategic economic importance, trade secrets misappropriation is the only form of U.S. intellectual property violation for which the owner lacks access to federal court. This leaves U.S. firms without a key tool to prevent trade secret theft and recover any losses.

Access to federal courts is critical for businesses of all kinds. State civil trade secret laws alone often are not sufficient to deter and remedy interstate theft. State courts are not always well suited to working quickly across state and national

<sup>&</sup>lt;sup>5</sup> Office of the Intellectual Property Enforcement Coordinator, <u>"Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,"</u> February 2013.

boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country. State laws can vary, making it harder for firms to craft consistent policies.

When a trade secret is stolen, its owner must act quickly to protect proprietary information and preserve evidence. Without access to federal courts, thieves have the advantage. For example, there are at least six airports with international flights within a two-hour drive from my facility in Baltimore. Five of those airports are in other states – New Jersey, Pennsylvania and Virginia. By the time multiple state courts take action, the criminals will be long gone.

Beyond any delays, taking civil action to protect trade secrets across multiple jurisdictions is also difficult and costly, particularly for small businesses. Unless small businesses have legal firms on retainer in different states, which most do not have, of course, they are effectively barred from using a key tool to defend their rights. That needs to change, and I urge the Judiciary Committee to act swiftly on legislation providing access to federal courts for trade secret theft.

Finally, we must meet the global challenge of trade secrets theft with global solutions. The United States should make common cause with Europe, Japan and others around the world that are facing the same problems and beginning to pursue their own solutions. We need strong trade secret protection and enforcement commitments in America's trade agreements, including those under negotiation with Europe and 11 Pacific Rim nations.

With effective criminal protection and access to federal civil enforcement here at home, U.S. negotiators can work with our overseas partners to improve trade secret protection and enforcement and to foster collective action through our trade agreements. Our partners have a shared stake in the success of that endeavor. They should be eager to work with us and to contribute ideas and solutions from their own experience.

\* \* \* \* \*

Chairman Whitehouse, Ranking Member Graham and members of the Subcommittee, trade secrets are vital for manufacturers small and large. America's trade secrets laws and policies much keep pace with today's threats. Manufacturers need your help to ensure they can effectively and efficiently protect and enforce their trade secrets.

I applaud your attention to this critical challenge and your focus on solutions. With strong global partnerships, with closer collaboration between federal agencies and between government and business, and with improvements to U.S. laws, including access to federal civil enforcement, we can have a real impact.

Thank you for the opportunity to testify this afternoon. I look forward to answering any questions you may have.