



## PRESS RELEASE

# Russian International Money Launderer Arrested for Illicitly Procuring Large Quantities of U.S.-Manufactured Dual-Use Military Grade Microelectronics for Russian Elites

Monday, September 18, 2023

**For Immediate Release**

Office of Public Affairs

Maxim Marchenko, 51, a Russian citizen who has resided in Hong Kong, was charged today in connection with conspiring to defraud the United States and with smuggling, wire fraud, and money laundering offenses based on his alleged participation in a scheme to unlawfully procure U.S.-sourced, dual-use microelectronics with military applications on behalf of end users in Russia.

“According to the complaint, Marchenko employed a web of shell companies as part of an overseas smuggling ring to ship dual-use U.S. technology with military applications to Russia in contravention of U.S. law,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Today’s action reinforces the Department’s commitment to protect U.S. security and counter Russian aggression in Ukraine through the vigorous enforcement of our export control laws.”

“As alleged, Maxim Marchenko participated in an illicit procurement network that provided military grade microelectronics to end users in Russia,” said U.S. Attorney Damian Williams for the Southern District of New York. “Following Russia’s unjust invasion of Ukraine, Marchenko and his co-conspirators are alleged to have used shell companies and other deceptive measures in order to secure U.S.-manufactured microelectronics, with applications including in rifle scopes, night-vision goggles, thermal optics, and weapon systems, for use by Russians. This office will relentlessly pursue those who seek to flout U.S. law in order to supply Russia with military technology.”

“Today’s charges demonstrate the FBI’s ability to leverage its international presence and partnerships to stop the illegal transfer of dual-use technology to Russia,” said Executive Assistant Director Larissa L. Knapp of the FBI’s National Security Branch. “As alleged in the charges, Marchenko and his co-conspirators engaged in an elaborate, fraudulent scheme to smuggle military-grade technology with the potential to harm U.S. national security. The FBI and our partners will never waver in our commitment to keep Americans safe.”

“We are laser-focused on rooting out the procurement networks fueling the Russian war machine,” said Assistant Secretary for Export Enforcement Matthew S. Axelrod. “Working hand-in-hand with our federal law enforcement partners, we will continue to identify and disrupt Russia’s use of front companies in the People’s Republic of China and elsewhere to evade our controls.”

“Disrupting the efforts of facilitators and procurement agents like Marchenko, who use their skills and connections to advance the agenda of the Russian war machine, is one of the most important priorities of this task force. Today’s arrest should serve as another reminder that we will leverage and deploy every tool to bring these criminals to justice,” said Task Force KleptoCapture Co-Director David Lim.

According to court documents, Maxim Marchenko is a Russian national who resides in Hong Kong and operates several Hong Kong-based shell companies, including Alice Components Co. Ltd. (Alice Components), Neway Technologies Limited (Neway) and RG Solutions Limited (RG Solutions). Marchenko and two co-conspirators (CC-1 and CC-2), who are also Russian nationals, have operated an illicit procurement network in Russia, Hong Kong and elsewhere overseas. This procurement network has fraudulently obtained from U.S. distributors large quantities of dual-use, military grade microelectronics, specifically OLED micro-displays, on behalf of Russia-based end users. To carry out this scheme, Marchenko, CC-1 and CC-2 used shell companies based in Hong Kong and other deceptive means to conceal from U.S. Government agencies and U.S. distributors that the OLED micro-displays were destined for Russia. The technology that Marchenko and his co-conspirators fraudulently procured have significant military applications, such as in rifle scopes, night-vision goggles, thermal optics and other weapon systems.

To perpetrate the scheme, Marchenko and other members of the conspiracy acquired the dual-use OLED micro-displays from U.S.-based distributors using Marchenko’s Hong Kong-based shell companies, including Alice Components, Neway and RG Solutions. Members of the conspiracy, including Marchenko, procured these sensitive microelectronics by falsely representing to the U.S. distributors (who, in turn, are required to report to U.S. agencies) that Alice Components was sending the shipments to end users located in China, Hong Kong and other countries outside of Russia for use in electron microscopes for medical research. In reality, the OLED micro-displays were destined for end users in Russia. Marchenko and other members of the conspiracy concealed the true final destination (Russia) from U.S. distributors for the purpose of causing false statements to the U.S. agencies.

To conceal the fact that these OLED micro-displays were destined for Russia, Marchenko and other members of the conspiracy worked together to transship the illicitly procured OLED micro-displays by using pass-through entities principally operated by Marchenko in third countries, such as Hong Kong. Marchenko then caused the OLED micro-displays to be shipped to the ultimate destination in Russia using, among other entities, a freight forwarder known to provide freight forwarding services to Russia. In addition, Marchenko and other members of the conspiracy used Hong Kong-based shell companies, principally operated by Marchenko, to conceal the fact that payments for the OLED micro-displays were coming from Russia. In total, between in or about May 2022 and in or about August 2023, Marchenko’s shell companies funneled a total of more than \$1.6 million to the United States in support of the procurement network’s efforts to smuggle the OLED micro-displays to Russia.

Marchenko is charged with conspiracy to defraud the United States, which carries a maximum penalty of five years in prison; conspiracy to commit money laundering, which carries a maximum penalty of 20 years in prison; conspiracy to smuggle goods from the United States, which carries a maximum penalty of five years in prison; money laundering, which carries a maximum penalty of 20 years in prison; smuggling goods from the United States, which carries a maximum penalty of 10 years in prison; conspiracy to commit wire fraud, which carries a maximum penalty of 20 years in prison; and wire fraud, which carries a maximum penalty of 20 years in prison. A federal district court judge will determine any sentence after considering the U.S. sentencing guidelines and other statutory factors.

The FBI and Commerce Department's Bureau of Industry and Security are investigating the case. The FBI Legal Attaché in Australia; U.S. Department of State's Diplomatic Security Service (DSS); and the Justice Department's Office of International Affairs provided valuable assistance.

The Southern District of New York is prosecuting the case, with assistance from the National Security Division's Counterintelligence and Export Control Section.

Today's actions were coordinated through the Justice Department's Task Force KleptoCapture and the Justice and Commerce Departments' Disruptive Technology Strike Force. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia's unprovoked military invasion of Ukraine. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation states.

*A criminal complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.*

[Marchenko complaint](#)

*Updated September 20, 2023*

## Topics

COUNTERING NATION-STATE THREATS

EXPORT CONTROL

## Components

[Criminal - Office of International Affairs](#) | [Federal Bureau of Investigation \(FBI\)](#) | [National Security Division \(NSD\)](#) | [Office of the Deputy Attorney General](#)

Press Release Number: 23-1018