SECURING THE FUTURE: HARNESSING THE POTENTIAL OF EMERGING TECHNOLOGIES WHILE MITIGATING SECURITY RISKS

TESTIMONY OF RON GREEN
EXECUTIVE VICE PRESIDENT & CHIEF SECURITY OFFICER
MASTERCARD INTERNATIONAL INCORPORATED

Before the
United States House of Representatives Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

June 22, 2022

Good afternoon, Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee. My name is Ron Green, and I am Executive Vice President and Chief Security Officer of Mastercard. In this role, I am responsible for the cybersecurity of our network and operations as well as the physical security of Mastercard and its assets.

In addition to my role with Mastercard, I serve in several positions with government and industry groups coordinating private sector awareness of and responses to cyberthreats.

- I am Chair of the Financial Services Sector Coordinating Council (FSSCC).[1]
- I am Chairman of the U.S. Secret Service Cyber Investigation Advisory Board (CIAB).[2]
- I am Vice Chair of the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) and subcommittee Chair for the Transforming Cyber Workforce study. [3]

[1] The FSSCC was established in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry. The FSSCC is an industry-led non-profit organization and its mission is to bring together members from financial services, trade associations, and other industry leaders to assist the sector's response to natural disasters, threats from terrorists, and cybersecurity issues of all types. The FSSCC partners with the public sector on policy issues to enhance the security and resiliency of the U.S. financial system. The U.S. Department of Homeland Security recognizes the FSSCC as a member of the Critical Infrastructure Partnership Advisory Council on behalf of the banking and finance sector.

[2] Established in September 2020, the CIAB is an investigations-focused federal advisory committee, dedicated to providing outside strategic guidance to shape the Secret Service's investigative efforts in cybercrime and cyber-enabled fraud. As chair, I head the 16 member CIAB, composed of senior executives and experts from industry, government and academia. The goal of the CIAB is to provide outside strategic direction to the Secret Service's investigative mission. This includes helping the Secret Service identify the latest cybercrime, technology and policy trends, providing guidance as the agency looks to modernize their training, partnerships and investigative priorities. All CIAB members are appointed by the Department of Homeland Security secretary through the Secret Service director. Members serve in a volunteer capacity for two years with an opportunity to renew their membership for up to three years. The CIAB meets twice a year, unless requested by the Secret Service director.

[3] The CISA Cybersecurity Advisory Committee is a 22-member committee that operates as a board of industry and state, local, and tribal government leaders who advise the CISA Director on policies and programs related to CISA's cybersecurity mission.

- I am also a member of the Aspen Cybersecurity Group.[4]

I am here today to discuss the security implications of emerging technologies, actions that Mastercard takes to forecast and mitigate cyberthreats against these emerging technologies, efforts Mastercard participates in to enhance collaboration with industry and government partners to promote cybersecurity and resiliency, and recommendations for Congress to further secure and enhance the resiliency of the digital ecosystem from future cyberthreats. Many of the topics that I will discuss today are part of Mastercard's resiliency planning – things that Mastercard needs to comprehend to be ready to guard against strategic surprises and are practices we encourage to be adopted more widely by both public and private sector actors at home and abroad.

Background on Mastercard

Mastercard is a technology company in the global payments industry that connects consumers, financial institutions, merchants, governments, digital partners, businesses, and other organizations worldwide, enabling them to use electronic payments instead of cash and checks. We make payments easier and more efficient by providing a range of payment services using our family of well-known brands, including Mastercard®, Maestro®, and Cirrus®. We are a multi-rail network (debit, credit, prepaid and real-time payments) that offers customers one partner for their domestic and international payment needs.

Our payment solutions offer customers choice and flexibility to ensure security for the global payments system. Mastercard seamlessly processes more than 110 billion payments annually. With more than 2.9 billion cards issued through our family of brands globally, Mastercard serves consumers and businesses in more than 200 countries and territories.

Through our global payments network built over decades, which we refer to as our core, we "switch" (i.e., authorize, clear, and settle) payment transactions and deliver products and services. We also supply payment capabilities that include automated clearing house transactions (both batch and real-time account-based payments). Moreover, we provide integrated value-add cyber and intelligence products and solutions, information analytics and other security consulting services.

As a global organization with a far-reaching network, we are responsible for securing our organization, protecting our sector and helping to protect the trust and confidence that people have in the broader global ecosystem. We safeguard consumer data, protect points of connection and take a forward-looking approach towards mitigating risks facing the digital world today and those it will encounter tomorrow.

The State of Cybersecurity Today and the High-Stakes Losses from Cyberattacks

The world in which we are living today looks different than it did just a few years ago. Technology is continuing to evolve. It is connecting the disconnected and making our lives more convenient. The world was already rapidly moving toward a digital-first way of life, which has

[4] The Aspen Institute gathers diverse, nonpartisan thought leaders, creatives, scholars and members of the public to address some of the world's most complex problems. But the goal of these convenings is to have an impact beyond the conference room. They are designed to provoke, further and improve actions taken in the real world.

only been accelerated by the COVID-19 pandemic. How people shop, pay and interact is changing. Consider the following:

- In 2020, 2.5 quintillion bytes of data were generated per day by people and their devices.[5]
- As of January 2021, there were 4.66 billion active Internet users around the world, which is close to 60% of the world's population.[6]
- It is estimated that digital commerce transaction values will total $18 trillion by 2024.[7]
- By 2024, 50% of the world is expected to be using digital wallets[8]

But as interactions go digital, criminals follow. Supercharged attacks are becoming more common, indiscriminate and sophisticated. National infrastructure, healthcare research and government services are all being targeted.

The cost of global cybercrime is projected to reach $10.5 trillion annually by 2025. But the consequences for businesses go beyond the immediate financial loss. There is potential damage to users' trust. With so many connections, it is more important than ever for all of us to maintain trust throughout the digital ecosystem.

The constantly growing interconnected spider web of digital devices and services means that the problem is only going to grow. Tapping into all the digital economy has to offer results in creating more data – therefore, more to protect. Organizations or individual actors can no longer invest in cybersecurity systems that only offer protection for their own operations. The public and private sector must invest in the right foundations and guardrails that create a long-term, sustainable shield around the whole supply chain.

Mastercard Leads on Security and Privacy

Mastercard secures trust in the modern digital economy. Consumers and businesses are expanding their online interactions beyond cards and payments, significantly increasing information exposure risks and creating more potential vulnerabilities for cybercriminals to exploit. As such, Mastercard is investing in innovative technologies to secure digital interactions more comprehensively. We rolled out chip card technology across the U.S. and have committed to phasing out the magnetic stripes on newly-issued cards. We are now tokenizing transactions, shifting away from static data that can easily be stolen or replicated and replacing it with dynamic data. All this is supported through our use of real-time analytics to detect fraudulent activity every time you use your card. In recent years, we have also introduced security technologies such as Mastercard Safety Net, Mastercard Identity Check, our Mastercard Biometric Card, and ID Theft Protection. These innovations, which come at a significant cost,

[5] Jacquelyn Bulao, Techjury, *How Much Data is Created Every Day in 2022?* (Jun. 3, 2022) (citing Domo), available at: https://techjury.net/blog/how-much-data-is-created-every-day/#gref.
[6] *Id* (citing Statista).
[7] Juniper Research, Digital Commerce Key Trends Sectors and Forecasts 2016-2020.
[8] Juniper Research, Digital Wallets- Deep Dive Strategy & Competition 2019-2024.

produce real results. For example, our SafetyNet technology stopped real-time fraud attacks and prevented more than $10 billion in potential fraud in 2021 alone.

Mastercard's cybersecurity efforts are evolving with the ecosystem. We are focused on building security for all other types of transactions – enabling consumers and businesses to benefit from years of learning and development entrenched in our network security solutions. As an example, we must ensure the validity of a website within the cyber realm so that a payment in the digital payments space can go through intelligent decision-making. By expanding to new types of transactions, we are focused on growing existing security for customers, consumers and businesses – not only to keep them safe but also as a means of making their digital lives easier. Another objective is to ensure the stability of the system itself by reducing systemic risk.

Many aspects of the digital world are intertwined and dependent on one another. In undertaking these steps, we hope to build trust from participants in the system. This is not a responsibility that we take lightly. We take a multi-layered, principled approach to cybersecurity that enables us to work extensively with emerging technologies while using cutting edge tactics to comprehend threats and guard against strategic surprise.

Privacy is central to securing trust in the modern digital economy, but there is a major trust deficit in how organizations and governments collect, use, and share people's data. At Mastercard, we embrace a strong, individual-first view of Privacy and Data.

We have instilled a Privacy By Design culture and mindset in our people. This looks like keeping privacy in mind from ideation through development and delivery of a product. There are multiple layers of privacy and security safeguards embedded into the design of our innovations to protect people's data – including through tokenization, encryption and anonymization. We only collect the information we need to get the job done. Moreover, we have extended GDPR's high standards and privacy rights to all individuals around the world.

Further emphasizing our commitment to the responsible use of data, we have established data responsibility principles establishing our vision of how data should be managed. When it comes to your data, you're at the center. You own it. You control it. You should benefit from the use of it, and we protect it. While we use data to help businesses, governments, the public sector and individuals better understand the world around them through identifying trends and insights, we anonymize and aggregate it to maintain our privacy and security standards. We also leverage these trends and insights for social good, helping us to advance financial inclusion and global humanitarian efforts.

Threatcasting

I would like to discuss one particular tactic that has become an important part of our resilience planning and ability to anticipate future threat trends, Threatcasting. There are several government entities, including the U.S. Army and the U.S. Secret Service, that also leverage the Threatcasting process. I would encourage both public and private entities to also adopt Threatcasting as part of their own resiliency planning.

Threatcasting is threat forecasting. Traditionally, organizations think about their outlook on a one-, three-, or five-year horizon. With Threatcasting, Mastercard looks beyond those horizons, and we challenge ourselves to think 10 years ahead. This approach offers us a process to

combine a wide range of inputs and exercises to imagine a broad range of future threats. It also gives us a systemic way to look backwards from these imagined future dates to understand the steps needed to disrupt, mitigate and recover from future threats.

To bring this to life, we partnered with noted futurist Brian David Johnson. We gathered a group of global, public-private sector subject matter experts that represent a wide variety of cultural, sociological, economic and scientific fields. Like business planning, Threatcasting is something Mastercard does annually. This gives us a chance to build on our relationships, our thinking and our ideas year after year. It is important to highlight that we are not thinking about only one singular Future with a "capital F." We are thinking about multiple futures involving different types of people across the world, and we repeat this thought process multiple times. Then we can step back and ask: "What do we need to as an organization, as a nation and as an industry to prepare for those futures?"

We have used Threatcasting to forecast potential futures involving emerging and disruptive technologies like quantum, IoT and artificial intelligence (AI). Threatcasting helps us understand these technologies and the overlap between them. In the next decade, the adoption of emerging technologies will expose greater vulnerabilities that will allow criminals, nation-states, corporations, organizations and individuals to capture data (physical, digital, biological) and whole identities to commit fraud. Opportunities for fraud will increase and the motivation to commit this type of crime will grow. Beyond financial gain, the perpetrators will have political and ideological goals, co-opting criminals, proxy attackers and unsuspecting combatants as allies.

Some of the highlights at the intersection of fraud, cyberattacks and emerging technology from past Threatcasting exercises include:

- The New Criminals: In this future, criminals use emerging autonomous technologies like AI, IoT, smart cities and cloud computing to evolve their tactics resulting in the development of a cybercrime economy to monetize these advances.

- Hiding in the Complexity. In this future, criminals will use the expanding technological landscape to commit traditional fraud by hiding in the complexity and scale of the technology, business and financial ecosystems. Think about it as "Old Fraud in New Ways."

- New Motivations. In this future, bad actors will use traditional fraud and broader criminal activities for nontraditional effects, attacking beyond financial systems to adjacent infrastructure. The logic of these attacks will be orthogonal to traditional attacks with expanded goals to destabilize, distract, disrupt, influence and just to prove it is possible. Think of this future as "New Fraud in Old Ways."

- Pandemic Problems: When the COVID-19 pandemic took hold of the globe, we convened a special session to Threatcast from a pandemic perspective to specifically look at effects on Mastercard's business operations. In 10 days, we were able to deploy teams to address potential vulnerabilities identified using this method.

Threatcasting is not something we have kept to ourselves at Mastercard. It can be a truly global exercise because we are invested in building a global digital ecosystem that is secure and connected. We have partnered with others across the financial sector to collaborate on Threatcasting. In my role as Chair of the FSSCC, I worked to combine the results from Mastercard's Threatcasting process with additional insights drawn from members across the financial services sector to further develop a comprehensive view of the threat landscape. Through these partnerships, we can provide a more complete picture of what we expect lies ahead. Mastercard has also shared our Threatcasting process with the G-7 Cyber Experts Group, a group of cybersecurity experts from G-7 nations that meets regularly to facilitate progress on major international debates and reports their findings to G-7 ministers and governors.[9]

The Current Threat Landscape

I would like to highlight for the Subcommittee some of the key future threats that we see, which require public and private sector action to mitigate future losses. Using the insights gained from our Threatcasting process as well as through our partnership engagements, there are six key topic areas I would like to discuss.

1. Global Ground Systems to Space-Based Asset Attacks. In the next decade, the expansion of Financial and Communications Critical Infrastructure (FIN/COM CI) from global ground systems to satellites will generate a unique set of future conditions that will multiply the scope, scale and speed of attacks, taking advantage of rising privatization and militarization as well as undermining situational awareness of the operating environment. The attack surface will no longer be "Earth" global, they will be "universe" global. A new set of evolving future threats will rise from these conditions, taking advantage of threat multipliers with rapid cascading effects and advancing FIN/COM CI as a minimum viable target for nation-states. These FIN/COM CI consumer-centered attacks will have a destabilizing chain reaction across systems and markets, leaving attribution nearly impossible and retaliation an unlikely option. The actors in the primary threat futures were the usual suspects: criminals, lone wolves and state-sponsored attacks. However, we determined that the goal of their threats will not be for financial gain. Instead, the aim of their attacks will be to destabilize industries, consumers and governments via loss of confidence and trust to the advantage of criminals, businesses and geopolitical actors. In some consumer-centric cases, the goal may even be to incite civil and business chaos.

2. Mis-, Dis-, Mal-information to Cause Instability. Mis-, dis-, and mal-information (MDM) is a rapidly emerging tactic for threat actors. Together, these three areas make up what CISA defines as "information activities." MDM campaigns promote geopolitical instability, which amplifies destabilizing events. Large-scale destabilizations like fuel, energy, food or water shortages can lead to financial fear and cause consumer panic. Overall, MDM campaigns have the potential to radicalize people, ultimately driving an increase in global geopolitical tensions while heightening the risk of insider threat and undermining trust. Building trust with stakeholders takes time, but it will help to build

[9] *See* https://www.cyberseek.org/heatmap.html

resiliency. However, resiliency efforts at all levels cannot be successful if people lack trust in the digital ecosystem, and MDM campaigns actively work to undermine that. From a technological standpoint, this can take different forms: (i) enhancing trust framework, inclusive of the hardware and software that is used; and (ii) implementing solutions like digital identity and zero trust frameworks that use methods to authenticate and verify that people are who they claim to be.

3. Workforce Shortages. There are three workforce-related threats that I would like to highlight:
    - First and foremost, there are not enough cybersecurity professionals. Currently, there are just under 715,000 open cybersecurity jobs within the U.S., and this gap is rapidly increasing.[10] For reference, in May 2021, there were approximately 465,000 cybersecurity job openings.[11] Strong cybersecurity professionals require a mix of soft and technical skills, which makes cyber recruitment unique and more difficult. In my work as Vice Chair of CSAC, I lead the Subcommittee focused on "Transforming the Cyber Workforce." That Subcommittee is in the process of finalizing and voting on a series of recommendations that we believe will help begin to address this problem.
    - Second, we need to think through – and work to mitigate – risks that come with our new normal of distributed workforces. The COVID-19 pandemic drove an adoption of hybrid work that is here to stay. It may look slightly different in various companies and cultures, but at the end of the day, the workforce has proven that this is a viable operating model. While it brings some positives, it also presents a real challenge from a security perspective. Managing a distributed workforce means needing more complex solutions and enabling access to more things that exist outside of an organization's security perimeter. The more points of connection that live beyond that perimeter, the greater the security risks. In a distributed workforce, the attack surface is greater.
    - Third, within the current workforce, corporate organizations are seeing a rise in Insider Threat. Insider Threat is a malicious threat to an organization that comes from the people with access to privileged or protected information. It takes two primary forms: intentional and unintentional. Intentional Insider Threat is when someone knowingly, for a variety of motivations, misuses their own access to the organization's confidential information or trade secrets or its customers' data to deliberately share them on an unauthorized basis outside of the organization. Unintentional Insider Threat has the same result, but the employee is fooled through naivete or lack of conscious attention into falling for social engineering, phishing or other similar tactics. Thus, the unauthorized access does not arise from the same motivations.

4. Cybercrime for Hire. As the "cybercriminal workforce" evolves, so do its tactics. We are in the midst of a rapid expansion of cybercrime as a service. As such, participation in

[10] *See* https://www.cyberseek.org/heatmap.html.
[11] Kristopher J. Brooks, CBS News Moneywatch, *U.S. has almost 500,000 job openings in cybersecurity* (May 21, 2021) (citing Cyber Seek), available at: https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/.

cybercrime does not require any technical competency. In fact, the barrier to entry is low. The target can be identified and a simple email sent with nefarious content. Through cybercrime-as-a-service offerings, it is now possible to purchase turnkey criminal solutions, pay for cybercrime to be conducted on one's behalf, or enlist cybercriminals to use the technology, tactics and procedures that allow the exploitation of vulnerabilities in a system that have been disclosed but not yet fixed, known in the industry as "zero-day vulnerabilities." In addition to these external services, insider access to organizations can be bought for nefarious use and ransomware gangs continue to offer ransomware as a service. This growth of "cybercrime for hire" underscores the importance of cyber hygiene, the practices and procedures that are regularly performed to maintain the security of users, devices, networks and data. Good cyber hygiene can help mitigate the increased risk that has resulted from this outsourcing of cybercrime.

5. Coordination Between Threat Actors and Foreign Governments. The intersection between the worlds of cybercriminals and nation-state operators will continue to grow. Whether deliberate or not, cybercrime is becoming a shared exercise between criminals and rogue nations. These lines, while once relatively clear, have become blurred. The world has seen increased geopolitical tensions give rise to more malicious cyberactivity. Complicating this is the fact that threat actors are both acting independently and at the behest of nation states. Attribution, while difficult before, is now nearly impossible. It has become incredibly challenging to discern when hackers are acting on their own interest or when they are carrying out an attack on behalf of nation-states.

6. Supply Chain Threats. There are three supply chain-related threats that I would like to highlight for you today:
    - COVID-19 has created an immature microcosm of small businesses that established themselves due to economic need and to meet a changing customer commercial demand for goods and services. Such businesses were set up quickly and at low cost, which meant cybersecurity was often not top of mind. We are seeing small businesses that don't understand cyber threats and lack an understanding of the basic mitigations. As a result, they are falling victim to preying criminals who are aware of their naivete and immaturity.
    - Separately, it has also become essential for organizations to be mindful of whom they are doing business with and where they are doing business. Consider the recent PAX point-of-sale terminals incident, for example. That situation demonstrates the importance of knowing the source of software as well as the location of data storage.
    - Organizations are also increasingly relying on the supply services of others, including small businesses, to make their businesses function (e.g. hosting providers, marketeers, digital cooling systems or distributors). These are services that require connectivity to their digital network but don't have control of the network. These 3rd, 4th and Nth party services within the supply chain create a weakness that is readily exploited and can create mass digital casualties globally through this one business/vulnerability. This is a particularly acute risk for municipalities in the U.S. A recent RiskRecon report on the state of cybersecurity

in the 271 largest U.S. cities revealed that 110 of the 271 cities may have security gaps present in their systems that could potentially result in data compromise.[12] This concept highlights the importance of understanding where our critical nodes and concentration risks are when it comes to national critical infrastructure. The SolarWinds supply chain compromise demonstrates the potential devastation that can come with the exploitation of critical nodes.

7. The Rise of Nationalism Fuels Divisions in the Global Digital Ecosystem: Cross-border payments play a critical role in the global economy. Each step of a transaction—from capturing, to processing, to authorizing a payment—relies on data, making the free flow of data a critical prerequisite for a functioning international payments ecosystem. Unfortunately, data localization policies around the world have more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration. These restrictions introduce a new level of complexity to the ecosystem and how organizations work to secure it. They require more data centers in more places, reducing efficiency and driving up costs as organizations work to maintain regulatory compliance. Data localization also fragments cybersecurity, broadening the attack surface for bad actors, limiting the scope of what organizations can see and making threat analysis and detection much more complex. Global digital standards that are yet to be written are an issue of cybersecurity. Every time we ignore a country that promotes on-soil requirements, the ecosystem becomes more fragmented and the ability of like-minded governments to ensure effective cybersecurity is weakened.

Mastercard's Partnerships to Bolster Cybersecurity

Mastercard engages in partnerships with governments, academia and the private sector from around the world to secure the entire global digital ecosystem from threats. Threats come from all parts of the world and are often not isolated to a region. Opportunities exist for the industry to work closely with government partners both domestically and internationally. The cyber threat requires like-minded organizations and governments to work together as one unit and use our shared expertise to defend ourselves in the future. It requires the use of creative, bold and broadly beneficial ideas. Mastercard supports the sharing of intelligence and best practices across the public and private sectors around the world to drive detection, response and interoperability of cyber defense practices.

I would like to express our company's appreciation in the U.S. for the role that CISA has played in leading the effort in collaborating with the private sector to enhance the security, resiliency and reliability of the nation's cybersecurity and communications infrastructure.

The financial services sector also appreciates the role that the U.S. Treasury plays as our Sector Risk Management Agency (SRMA). Treasury supports our sector to ensure that CISA receives accurate, comprehensive information about current sector operations and any potential incidents.

[12] Riskrecon, *Report: The state of cybersecurity in U.S. cities* (February 2022), available at: https://www.riskrecon.com/report-the-state-of-cybersecurity-in-us-cities.

Treasury coordinates with the sector and CISA to identify sector risks and then assesses and mitigates them by conducting regular exercises to test preparedness and emergency planning.

Additionally, Mastercard participates in domestic and international cybersecurity exercises such as the North Atlantic Treaty Organization's Locked Shields and CISA's Cyber Storm. We are active contributors in the Financial Services Information Sharing and Analysis Center (FS-ISAC) and participate in sector-specific and multi-sector cyber defense exercises and information sharing efforts. Mastercard also organizes and hosts its own cyber defense exercises for the financial services sector and the broader tri-sector community (including the financial services, energy and telecommunications sectors). To provide a snapshot of some of our global cybersecurity partnerships, we:

- Engage with the European Cyber Resilience Board, European Cyber Crime and Fraud Investigators, Europol, INTERPOL, National Cybersecurity Authority and the National Cyber Security Center to share cyber threat intelligence and build a more secure digital ecosystem with partner communities.

- Co-lead the Financial Services Cyber Collaboration Center (FSCCC) in the U.K. with daily meetings with our partners to identify systemic risks to the financial sector.

- Partner with the National Cyber Forensics and Training Alliance (NCFTA) to collaborate and combat cybercrime and fraud.

- Collaborate with the Dubai International Finance Center to strengthen the cybersecurity of more than 3,000-plus financial institutions in the region.

- Support the Global Cyber Alliance, Cyber Readiness Institute, National Cyber Security Alliance and Small Business Development Centers (SBDC) to equip small and mid-size businesses with free cybersecurity toolkits, education and training.

- Strengthen workforce development, education and training through our work with the National Institute of Standards and Technology (NIST) and the National Initiative for Cybersecurity Education (NICE) community to ensure our workforce is prepared for today's threats, as well as those threats we will face in the future.

Mastercard has centers of cyber innovation around the world:

- The Intelligence & Cyber Centre of Excellence is in Vancouver, Canada. The Centre was created in partnership with the Government of Canada through its Strategic Innovation Fund, with an additional $510 million investment by Mastercard. Opened in 2022, the Centre is leading innovation in cyber and intelligence, AI and the IoT. Research from the Centre is already enhancing Mastercard solutions, and combining the Centre's biometric security algorithms with existing cyber capabilities is creating new approaches to enhance online security.

- In partnership with EnelX and the Government of Israel, Mastercard opened the FinSec Innovation Lab in Beer-Sheva, Israel in 2021 to advance innovations in Israel in financial technology and cybersecurity for the payments and energy ecosystem globally. The Lab partners with Israeli startup companies to test and develop products and solutions, with a particular focus on cybersecurity and digital security, among other fields.

- Mastercard established a European Cyber Resilience Centre in Waterloo, Belgium in 2020. The Centre drives collaboration between both public and private sectors as well as regulatory bodies to further support enterprise resilience in the region. The Centre highlights Mastercard's ongoing commitment to addressing threats faced by the European payments ecosystem, including financial institutions and fintechs. The facility serves as a single cybersecurity hub for the region, bringing together a diverse pool of talent from across Mastercard's global community. The Centre works with various cyber intelligence centres, industry groups, law enforcement agencies and central banks across Europe and helps drive better prevention and mitigation practices against international cybercrime and wider security threats.

- Mastercard established a Fusion Center in St. Louis, Mo. The Fusion Center leads and synchronizes Mastercard global resources to anticipate, identify and mitigate fraud and cyber and physical security threats or events requiring a joint response in order to protect Mastercard and contribute to the financial ecosystem's security.

- Mastercard established a DigiSec Lab in England to proactively test threats to all forms of digital payments in coordination with government security agencies and leading academics. This team deconstructs technology and identifies opportunities to strengthen it and continue to protect consumers, merchants and financial institutions from fraud. The team also works in close partnership with other groups to deliver a multi-layered approach to address security risks and concerns in digital payments.

- Mastercard operates tech hubs in Sydney, Australia; St. Louis, Mo.; New York City; Arlington, Va.; Dublin, Ireland; and in Pune and Vadodara, India.

Policy Recommendations

I would like to offer some cybersecurity policy recommendations for Congress that would strengthen the U.S. and global resilience against cyberthreats given current trends in emerging technologies:

1. Establish a National Cybersecurity Training Center within CISA. Congress should establish a National Cybersecurity Training Center (NCTC) within CISA, which would enable CISA and all critical infrastructure sectors to regularly coordinate and conduct live-fire cyber training sessions that give critical infrastructure owners and operators the chance to further partner with the government, their sector and cross-sector in putting their cyber defense and resiliency plans into action. Response plans and mitigation strategies are foundational to any organization's cyber posture, but those plans are

meaningless if critical infrastructure owners and operators have never executed them in real time under real circumstances. Right now, the opportunities for most organizations to undertake these tests as well as for cyber defenders to train so they are skilled against world-class and nation-state opposition forces are limited. But Congress can make these opportunities more widely available. The NCTC would be modeled after the U.S. Army's National Training Center, a large, live-fire and maneuver training area at Fort Irwin, Calif.

2. Create a National Cyber Academy. Congress should establish the National Cyber Academy (NCA), which would be mostly virtual but also a physical educational institution based on the current model for U.S. military academies. It could help build a strong cyber talent pipeline for both the public and private sectors. As discussed earlier, there are not enough cybersecurity professionals to fill all currently open roles, and this gap is only poised to grow over the next several years in both the public and private sectors. To help close this gap, I would propose the establishment of the NCA to help build a strong cyber talent pipeline based on common education and skill-based requirements. To address the needs of both the public and private sectors, the NCA would have two tracks: a traditional military academy-style CISA Cadet track and an open public-access track. The CISA Cadet track would mirror the traditional military academy processes and procedures, ending with a multi-year commitment to join CISA. This would enable CISA to have a consistent pipeline of well-trained staff to support CISA's mission as it continues to broaden in scope. The public-access track would give anyone the opportunity to enhance skills through certifications/classes that have been curated, vetted and widely accepted within the public and private sector. This would lower the barrier for entry to a cybersecurity career while giving people a clear path to demonstrate their cybersecurity knowledge without the need of a traditional four-year degree.

3. Develop within CISA a Cybersecurity Education Pathway Program. Congress should create a cybersecurity education pathway program within CISA that would help high school and college students build foundational cyber skills while increasing the visibility of cybersecurity as a career path and helping to develop a long-term, sustainable and scalable talent pipeline. Addressing the cyber workforce challenge requires not only filling the roles that are currently open but also taking steps to address the needs of tomorrow. This pathway would ultimately unify the many existing educational programs into one comprehensive development track built on the same infrastructure as the NCA (explained above). It would give students the ability to validate their cyber education in a way that is recognized and accepted by the private sector, making it simpler for them to begin their careers.

4. Establish a Tour-of-Duty Cyber Force Program within CISA. Congress should establish a tour-of-duty Cyber Force program within CISA. This program would bridge urgent talent gaps, enable the members of the cyber workforce to enhance their skills, and support ongoing efforts to deepen public-private collaboration. Security practitioners would volunteer for a one- to two-year tour of duty before returning to the private sector

and could serve as designated CISA liaisons to facilitate public-private threat sharing and collaboration during times of cybersecurity crisis. To further incentivize broad participation in this program, participating organizations would receive tax credits or other similar benefits.

5. Expand the Cybersecurity Talent Initiative. Congress should appropriate additional funding to expand the Cybersecurity Talent Initiative, a public-private partnership aimed at recruiting and training a world-class cybersecurity workforce. Through the Cybersecurity Talent Initiative, Mastercard and other private sector organizations partner with the federal government to cultivate cybersecurity talent for both the public and private sectors. In this unique program, participants serve two years in the federal government. Before the end of their federal service, participants are invited to apply for full-time positions with the program's private sector partners. By working for federal organizations and cutting-edge private sector companies, participants develop the skills and knowledge needed to protect our country's digital infrastructure and tackle cybersecurity threats.

6. Enhance Global, Sector-Agnostic Intelligence Sharing and Analysis with the Private Sector and Allied Governments. Congress should enhance CISA and the appropriate federal agencies' ability to create and participate in global, sector-agnostic intelligence sharing and analysis work with private sector participants and allied governments. Unlocking the shared ability to analyze incidents, review attack vectors and spot trends across sectors is key to the continued ability to defend against cyberattacks. Cybercrime is not constrained by borders, political jurisdictions or sectors. Threat actors attack targets around the world, using information gained along the way to improve their approach. The federal government and industry have limited intelligence-sharing capabilities that span the entire threat landscape. The digital ecosystem would be better equipped to defend itself if participants had enhanced capabilities to analyze incidents, review attack vectors and spot trends across sectors, geographies and governments.

7. Promote the Harmonization of International Cybersecurity Standards, Regulations and Risk Management Frameworks. Congress should adopt industry-led and internationally accepted standards, regulations and risk management frameworks to support global cybersecurity, digital trade, electronic payment services, fintech and emerging technologies. The world is witnessing record levels of cyberattacks and this is in part due to the lack of a global consensus to address systemic cybersecurity challenges. Policymakers should also collaborate with private sector leaders that have experience aligning industry-leading best practices and standards around current and emerging technology. Having multiple standards, regulations and risk management frameworks globally is unnecessarily complicated and costly to comply with due to the web of national and regional regulations. Under current cybersecurity requirements, companies must juggle many competing laws across jurisdictions. There are also conflicting definitions of what constitutes a cybersecurity incident and what should trigger a notification to regulators and consumers. This impacts interoperability and impedes open systems and innovation. The global harmonization of cybersecurity standards,

regulations and risk management frameworks would benefit industry and governments by lowering risk, reducing costs and furthering innovation. Thus, it is critical to foster partnerships among allied governments and the private sector that will help shape the standards, regulations and risk management frameworks that apply to cybersecurity.

8. Strengthen the Collaboration Between the Critical Infrastructure Owners and Operators and the Intelligence Community. Congress should direct CISA and the appropriate federal agencies to strengthen active and collaborative support and engagement between the intelligence community (IC) and critical infrastructure owners and operators on cyberthreats. Increased communication between the IC and industry is needed to better protect critical infrastructure. During an incident, there must be a continuous, real-time and bi-directional exchange of information.

9. Enable Trusted Data Flows and Privacy. Congress should work with the international community to remove discriminatory and protectionist barriers to data flows. In addition, countries should commit to recognizing the importance of setting standards on privacy, such as new Trans-Atlantic Data Privacy Framework, cybersecurity, and development of data governance frameworks.

* * *

Thank you for the opportunity to testify in front of the Subcommittee. Today's topics are critical to the future of our nation. The world we're living in today looks very different than it did at the start of the decade. The pace of change is only increasing and our shift to a digital-first world is rapid and irreversible. Understanding the current threat landscape and the impact of emerging disruptive technologies are essential to our successful shared resilience planning, ultimately helping us to guard against strategic surprise. I am happy to answer any questions from the Subcommittee.