Where is M³AAWG Headed in 2025 and Beyond

Sara Roper,
M³AAWG Chairperson
Janet Jones,
M³AAWG Expert Advisor

June 17, 2025

M³AAWG is a Trusted Environment

M³AAWG ENGAGEMENT SERIES

What happens in M³AAWG stays in M³AAWG

- What occurs here cannot be shared outside the membership without the written permission of the Executive Director, unless we state the specific session is open to the press and social media.
- See the M³AAWG Meeting Policy at www.m3aawg.org/MeetingPolicy

Treat Everyone with Respect

- Treat all attendees respectfully in and out of sessions. No less will be tolerated.
- See the M³AAWG Conduct Policy at https://www.m3aawg.org/conduct-policy

You agreed to these policies when you registered for the meeting.
For questions, please contact Amy Cadagin at amy@m3aawg.org

Reminders for Our Worldwide Friends

M³AAWG ENGAGEMENT SERIES

All meeting content is confidential: No photos, no video, no recording, No WireShark or exploration devices. Reach out to staff with questions.

Le contenu de toutes les rencontres est confidentiel. La prise de photos, vidéo ou enregistrements sont interdites, y compris les appareils d'exploration ou de type "wireshark". N'hésitez pas à contacter un des membres du personnel pour toutes questions.

Todo el contenido de la reunión es confidencial. No es permitido tomar fotos o grabar video. No es permitido usar Wireshark o dispositivos de captura o análisis de tráfico en la red. Diríjase al personal de M³AAWG si tiene preguntas.

Der gesamte Meetinginhalt ist vertraulich. Keine Fotos, kein Videos, keine Tonaufnahmen. Kein Wireshark oder Monitoring-Tools. Bei Fragen wenden Sie sich an das Team.

会議の内容はすべて機密扱いです。写真やビデオの撮影、録音，ワイヤーシャークや探索デバイスの利用は禁止されています。質問がある方は、スタッフまでご連絡ください。

所有会议内容均为保密信息：禁止拍照、录像、录音。没有 WireShark 或探索设备
如有疑问，请咨询职员。

모든 회의 내용은 기밀입니다. 사진 및 동영상 촬영, 녹음, 와이어샤크(Wireshark)와 같은 분석 툴의 사용을 금지합니다. 질문이 있으시면 직원에게 문의해 주십시오.

Вся информация о встречах конфиденциальна: никаких фотографий, видео, записей, WireShark или исследовательских устройств. Обращайтесь к персоналу с вопросами.

M3AAWG ENGAGEMENT SERIES

Sara Roper
M³AAWG Chairperson
Bank of America

M³AAWG
ENGAGEMENT SERIES

OUR VALUES

We Value CLARITY.

These are the core beliefs and guiding principles that shape how M³AAWG operates. It is our culture and internal compass for how we collaborate, interact with stakeholders, and direct our efforts.

C — COLLABORATION
We are in this together as a working group, driving real results through shared contributions and effort.

L — LEARNING
We invest in each other and grow by resourcing our members, communities, and partners through shared learning and support.

A — AWARENESS
We keep our eyes and minds open. We challenge assumptions, stay curious, and seek better solutions through inquiry, hypothesis, and a commitment to test, learn, and improve.

R — RESPONSIBILITY
We tackle the hard challenges with a commitment to progress, and hold ourselves accountable to solving issues which move us closer to a world free of online abuse.

I — INVESTED
We show up committed and invested in our cause. We invest our time and talent to deliver on our mission.

T — TRUST
We trust in the community and champion trust by embedding data identity and protection principles into everything we build, ensuring integrity across people, systems, and platforms.

Y — YOU BELONG HERE
We are committed to a community of inclusion, respect, and representation - where diverse voices are not only welcomed but vital.

M³AAWG ENGAGEMENT SERIES

We Value CLARITY

Collaboration

We are in this together as a working group, driving real results through shared contributions and effort.

M3AAWG ENGAGEMENT SERIES

We Value CLARITY

Learning

We invest in each other and grow by resourcing our members, communities, and partners through shared learning and support.

M³AAWG ENGAGEMENT SERIES

We Value CLARITY

C L A R I T Y

Awareness

We keep our eyes and minds open. We challenge assumptions, stay curious, and seek better solutions through inquiry, hypothesis, and a commitment to test, learn, and improve.

M3AAWG ENGAGEMENT SERIES

We Value CLARITY

Responsibility

We tackle the hard challenges with a commitment to progress, and hold ourselves accountable to solving issues which move us closer to a world free of online abuse.

We Value CLARITY

Invested

We show up committed and invested in our cause. We invest our time and talent to deliver on our mission.

M3AAWG ENGAGEMENT SERIES

We Value CLARITY

Trust

We trust in the community and champion trust by embedding data identity and protection principles into everything we build. This ensures integrity across people, systems, and platforms.

M³AAWG ENGAGEMENT SERIES

We Value CLARITY

You Belong Here

We are committed to a community of inclusion, respect, and representation - where diverse voices are not only welcomed but vital.

M³AAWG
ENGAGEMENT SERIES

OUR VALUES

We Value CLARITY.

These are the core beliefs and guiding principles that shape how M³AAWG operates. It is our culture and internal compass for how we collaborate, interact with stakeholders, and direct our efforts.

C — COLLABORATION
We are in this together as a working group, driving real results through shared contributions and effort.

L — LEARNING
We invest in each other and grow by resourcing our members, communities, and partners through shared learning and support.

A — AWARENESS
We keep our eyes and minds open. We challenge assumptions, stay curious, and seek better solutions through inquiry, hypothesis, and a commitment to test, learn, and improve.

R — RESPONSIBILITY
We tackle the hard challenges with a commitment to progress, and hold ourselves accountable to solving issues which move us closer to a world free of online abuse.

I — INVESTED
We show up committed and invested in our cause. We invest our time and talent to deliver on our mission.

T — TRUST
We trust in the community and champion trust by embedding data identity and protection principles into everything we build, ensuring integrity across people, systems, and platforms.

Y — YOU BELONG HERE
We are committed to a community of inclusion, respect, and representation - where diverse voices are not only welcomed but vital.

PRIORITIES AND FOCUS AREAS

As online abuse threats grow more advanced, M³AAWG is proactively evolving and adapting its work to meet emerging challenges, strengthening its organizational capabilities, expanding partnerships, and continuing to foster a diverse and inclusive culture.

Communications & Content

Securing the Conversation: Preventing, detecting, filtering, and stopping abuse in the content stream.

Detecting and blocking spoofed messages, lookalike domains, and impersonation attacks.

Preventing ransomware and malicious payload delivery via phishing, QR codes, and embedded links.

Mitigating abuse of trust and reputation through deceptive sender tactics.

Addressing AI-generated spam, phishing, and other content manipulation tactics.

Defending against evasion techniques designed to bypass filters and classifiers.

Platform & Infrastructure

Hardening the Stack: Addressing where abuse originates, scales, and evades detection.

Preventing abuse through compromised accounts, infrastructure, outdated cryptography, and other service misuse.

Detecting and mitigating fraudulent identity, platform, and account misuse.

Monitoring systemic threats targeting APIs, interfaces, and backend systems.

Identifying and mitigating abuse via malicious domains, botnets, open source, and insecure devices.

Evolving authentication protocols (e.g., SPF, DKIM DMARC, & MFA) to prevent abuse

User & Endpoint

Protecting the Edge: Focusing efforts where abuse lands, impacts users, and exploits trust.

Detecting and managing abuse across encrypted, proprietary, and other user environments.

DDoS command and control, amplification, and other DNS attacks.

Phishing tactics including QR codes, push notifications, and other mobile vectors.

Spoofing and fraud through biometric, authentication, and other novel techniques.

Device-centric credential threats: SIM swapping, MFA bypass, etc.

Policy & Regulations

Applying the Expertise: Establishing policies and practices, coordinating industry actions, and leading and adapting to global policy shifts.

Aligning operations with existing and emerging data privacy and cybersecurity regulations.

Enhancing transparency and accountability through policy and compliance.

Strengthening industry response capabilities through collaborative information sharing and partnerships.

Enabling effective industry coordination on opportunities, challenges, and threats.

Developing actionable abuse reporting standards and workflows.

M³AAWG ENGAGEMENT SERIES

M³AAWG *EVOLVED* PRIORITIES & FOCUS AREAS

PRIORITIES	FOCUS AREAS
Communications & Content ***Securing the Conversation:*** Preventing, detecting, filtering, and stopping abuse in the content stream.	• Detecting and blocking spoofed messages, lookalike domains, and impersonation attacks. • Preventing ransomware and malicious payload delivery via phishing, QR codes, and embedded links. • Mitigating abuse of trust and reputation through deceptive sender tactics. • Addressing AI-generated spam, phishing, and other content manipulation tactics. • Defending against evasion techniques designed to bypass filters and classifiers.

M³AAWG ENGAGEMENT SERIES

M³AAWG *EVOLVED* PRIORITIES & FOCUS AREAS

PRIORITIES	FOCUS AREAS
Platform & Infrastructure ***Hardening the Stack:*** Addressing where abuse originates, scales, and evades detection.	• Preventing abuse through compromised accounts, infrastructure, outdated cryptography, and other service misuse. • Detecting and mitigating fraudulent identity, platform, and account misuse. • Monitoring systemic threats targeting APIs, interfaces, and backend systems. • Identifying and mitigating abuse via malicious domains, botnets, open source, and insecure devices. • Evolving authentication (SPF, DKIM, DMARC & MFA) to prevent abuse.

M³AAWG ENGAGEMENT SERIES

M³AAWG *EVOLVED* PRIORITIES & FOCUS AREAS

PRIORITIES	FOCUS AREAS
User & Endpoint ***Protecting the Edge:*** Focusing efforts where abuse lands, impacts users, and exploits trust.	• Detecting and managing abuse across encrypted, proprietary, and other user environments. • DDoS command and control, amplification, and other DNS attacks. • Phishing tactics including QR codes, push notifications, and other mobile vectors. • Spoofing and fraud through biometric, authentication, and other novel techniques. • Device-centric credential threats: SIM swapping, MFA bypass, etc.

M³AAWG ENGAGEMENT SERIES

M³AAWG *EVOLVED* PRIORITIES & FOCUS AREAS

PRIORITIES	FOCUS AREAS
Policy & Regulation ***Applying the Expertise:*** Establishing policies and practices, coordinating industry actions, and leading and adapting to global policy shifts.	• Aligning operations with existing and emerging data privacy and cybersecurity regulations. • Enhancing transparency and accountability through policy and compliance. • Strengthening industry response capabilities through collaborative information sharing and partnerships. • Enabling effective industry coordination on opportunities, challenges, and threats. • Developing actionable abuse reporting standards and workflows.

PRIORITIES AND FOCUS AREAS

As online abuse threats grow more advanced, M³AAWG is proactively evolving and adapting its work to meet emerging challenges, strengthening its organizational capabilities, expanding partnerships, and continuing to foster a diverse and inclusive culture.

Communications & Content

Securing the Conversation: Preventing, detecting, filtering, and stopping abuse in the content stream.

Detecting and blocking spoofed messages, lookalike domains, and impersonation attacks.

Preventing ransomware and malicious payload delivery via phishing, QR codes, and embedded links.

Mitigating abuse of trust and reputation through deceptive sender tactics.

Addressing AI-generated spam, phishing, and other content manipulation tactics.

Defending against evasion techniques designed to bypass filters and classifiers.

Platform & Infrastructure

Hardening the Stack: Addressing where abuse originates, scales, and evades detection.

Preventing abuse through compromised accounts, infrastructure, outdated cryptography, and other service misuse.

Detecting and mitigating fraudulent identity, platform, and account misuse.

Monitoring systemic threats targeting APIs, interfaces, and backend systems.

Identifying and mitigating abuse via malicious domains, botnets, open source, and insecure devices.

Evolving authentication protocols (e.g., SPF, DKIM DMARC, & MFA) to prevent abuse

User & Endpoint

Protecting the Edge: Focusing efforts where abuse lands, impacts users, and exploits trust.

Detecting and managing abuse across encrypted, proprietary, and other user environments.

DDoS command and control, amplification, and other DNS attacks.

Phishing tactics including QR codes, push notifications, and other mobile vectors.

Spoofing and fraud through biometric, authentication, and other novel techniques.

Device-centric credential threats: SIM swapping, MFA bypass, etc.

Policy & Regulations

Applying the Expertise: Establishing policies and practices, coordinating industry actions, and leading and adapting to global policy shifts.

Aligning operations with existing and emerging data privacy and cybersecurity regulations.

Enhancing transparency and accountability through policy and compliance.

Strengthening industry response capabilities through collaborative information sharing and partnerships.

Enabling effective industry coordination on opportunities, challenges, and threats.

Developing actionable abuse reporting standards and workflows.

M3AAWG ENGAGEMENT SERIES

Alberto Pastor Nieto
M3AAWG Mobile Chair

Tanya Plaza
M3AAWG Mobile Chair

Janet Jones
M3AAWG Expert Advisor

M3AAWG ENGAGEMENT SERIES

Mobile Strategy

As we move deeper into the digital age, the landscape of fraud, phishing, and scams is evolving, especially within mobile environments. To better keep pace with the growing threats, M3AAWG has updated its Mobile strategy.

THE THREE FOCUS AREAS:

M3AAWG ENGAGEMENT SERIES

Mobile Communications

This includes various forms of communication via mobile devices—SMS, MMS, RCS, voice calls, and video conferencing apps. The primary threats here are scams, phishing, malware distribution, and intrusive marketing messages.

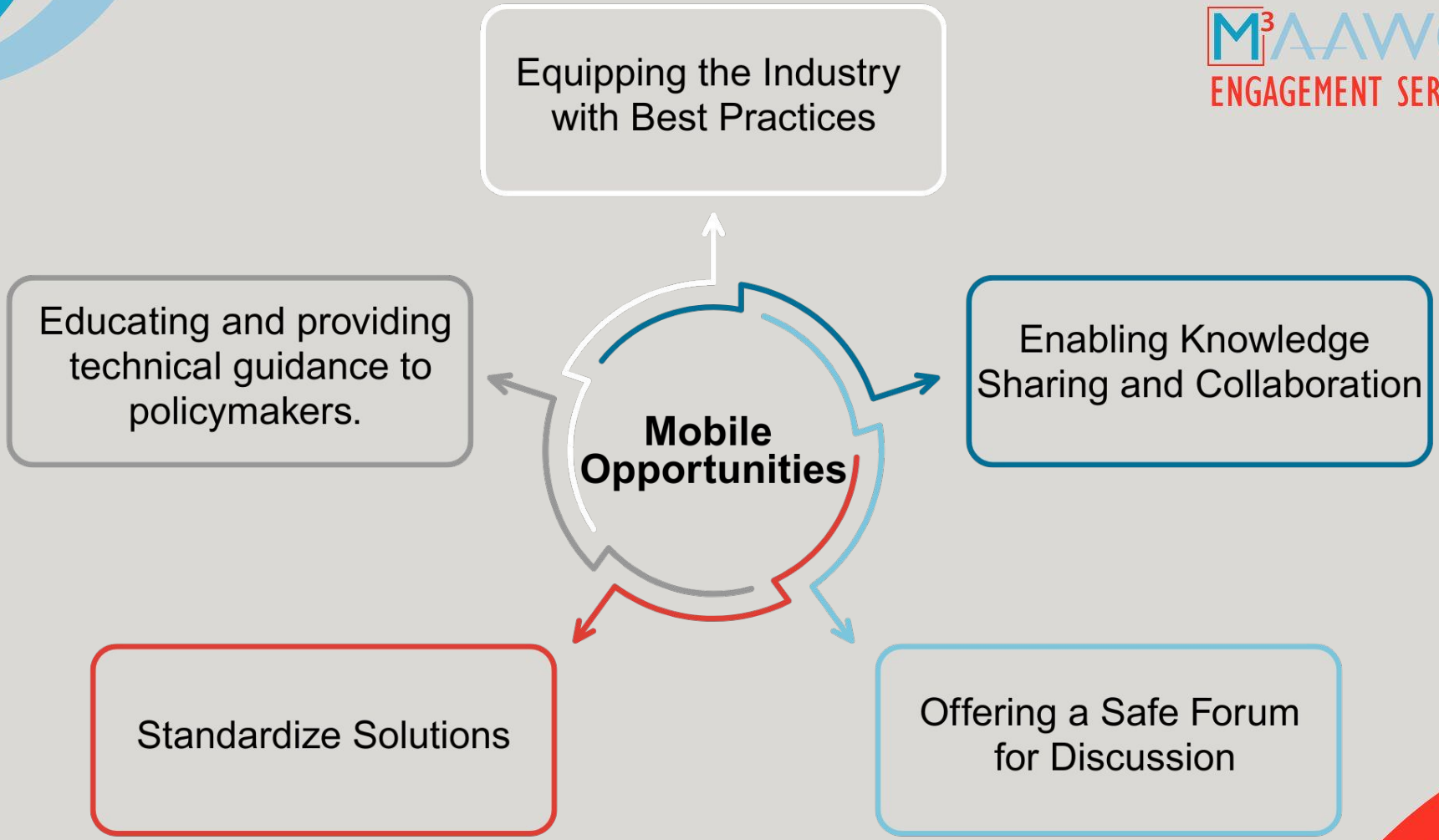
Mobile Devices

This subarea focuses on mobile operating systems (iOS, Android) and the actual devices from original equipment manufacturers (OEMs). The risks include malware, system vulnerabilities, and potential device hijacking.

Mobile Apps and Services

This encompasses a broad spectrum of applications that can be used to facilitate scams or become targets themselves (i.e., social media, banking apps, and gaming platforms).

M3AAWG ENGAGEMENT SERIES



M³AAWG Can Impact the Evolving Threat Landscape in Five Key Ways:

Equip the Industry with Best Practices:

Currently, the protection levels within the industry are inconsistent. By developing standardized best practices, M³AAWG can help equip businesses to combat fraud more effectively.

Enable Knowledge Sharing and Collaboration:

Scammers often exploit multiple platforms using similar techniques. Providing connection and establishing more collaboration among companies can help identify and combat these threats more proactively.

Offer a Safe Forum for Discussion:

M³AAWG provides a trusted forum environment to safely discuss problems and solutions, along with a collection of a broad spectrum of experts across the online industry.

Standardize Solutions:

The need for standardized solutions is more pressing than ever. M³AAWG can lead efforts to update and improve standards across the mobile ecosystem.

Educate Policymakers:

M³AAWG is committed to equip regulators by providing technical guidance and education on important regulatory matters impacting mobile.

M3AAWG ENGAGEMENT SERIES

CONTACT

For Priorities & Focus Areas:

Amy Cadagin, Executive Director, amy@m3aawg.org

For Mobile Strategy:

mobile-tech-chair@mailman.m3aawg.org