2024 LIFE INSURANCE & ANNUITY CONFERENCE

Powering Growth

Evolving Authentication Practices: Gold Standards For Identity Protection

LIMRA LOMA
Navigate With Confidence

SOCIETY OF ACTUARIES

ACLI
American Council of Life Insurers

Dan Vincent

Director, Financial Crime Unit

Price Waterhouse Coopers

Melissa Glynn

Head of Fraud Operations

MassMutual

Michael Kennedy

Senior Director

Equitable

LIMRA LOMA
Navigate With Confidence

SOCIETY OF ACTUARIES®

ACLI
Financial Security for Life

Emerging fraud trends require insurance firms to enhance their authentication capabilities

Fraudsters are continuing to evolve and defeat legacy authentication solutions.

Scams, including elder financial exploitation, continue to be key fraud schemes targeting consumers. These can be challenging for customers and institutions, as these are often considered “authorized” by the customer.

Trending account takeover frauds

I needed Tech Support for help, and they took control of my screen

IT Support Scammer

At Risk - The fraudster can find out personal identifiable information (PII) about the customer and later use the data to perpetrate fraud

At Risk - The fraudster can coerce the customer to log into their online account and request fraudulent disbursements

My daughter video called me and requested that I update my beneficiary designation

Scams Using Deep Audio and Video Fakes

At Risk - The fraudster can convince customers to change beneficiaries, request loans or other fraudulent distributions

I woke up this morning and someone had cashed out my insurance policy

Trusted Party Scams – external *and* internal

At Risk - The fraudster can exploit their position of trust and authority take advantage of vulnerable individuals

At Risk – Internal actors - employees at your firm may have fiduciary responsibility (e.g. annuities) and there is risk of abuse. Authentication can help stem this

LIMRA LOMA Navigate With Confidence

SOCIETY OF ACTUARIES

ACLI Financial Security for Life

Legacy processes are less resilient to new anti-MFA attacks; considerations to help mitigate account takeover

Traditional Multi-Factor Authentication (MFA) methods, including one-time passcodes (OTPs), push-based MFA, or text message-based MFA have grown outdated, leaving a gap for fraudsters to exploit technology particularly in the context of account takeover (ATO).

How fraudsters are defeating legacy authentication systems

1. **“MFA Prompt Bombing”**
   A newer technique as an attack method used to bypass MFA security by flooding users with MFA prompts to access a system, with the goal of finding a prompt that the user accepts.

2. **Issues with Push-based MFA and OTP**
   While convenient, push-based MFA is susceptible to human errors and potential unauthorized access if a device is compromised.

3. **Text Message-based MFA Vulnerabilities**
   A widely adopted authentication method that is susceptible to attacks (SIM-Swapping).

4. **Social Engineering**
   Fraudsters often use advanced tools, such as spoofed phone numbers, to act as the victim's trusted entity to gain access to the victim’s account(s).

Key considerations for mitigation

1. **Evaluate the risk landscape and assess the necessity of upgrading security to higher phishing-resistant standards**. Phishing attacks are becoming increasingly sophisticated, bolstering security measures is imperative

2. Phishing-resistant MFA solutions, such as **hardware tokens or biometric authentication, should be prioritized over OTP for internal systems and applications**. (Technology)

3. **Evaluate the risk level associated with these applications and upgrade security measures to a higher standard ("e.g. phishing-resistant").** Regular assessment of MFA measures can be essential to adapt to the evolving fraud. (Process)

4. Customers are often the weakest link. **Ramp up customer education and outbound awareness campaigns** so your customers can better recognize the risks that can lead them to being scammed. (Process)

LIMRA LOMA Navigate With Confidence
SOCIETY OF ACTUARIES
ACLI Financial Security for Life

Stronger authentication should be tightly linked and coordinated to broader fraud controls

Authentication does not typically exist in a vacuum, while insurance companies typically do not need as large a fraud program as banks, they should consider four key capabilities

Foundational Program elements...

1 Fraud Governance	**2** Fraud Technology and Data	**3** Fraud Analytics and Reporting	**4** Fraud Operations and Process
Lack of a holistic view of fraud threats and exposure	Challenges to measure and analyze current risks	Immature fraud or operational risk programs	Challenges to achieve single customer view	Increased sophistication of fraud attacks
Silos across functional teams/Lines of Defense	Increase in operating expense	Pressure from digital & payment transformation initiatives	Increase in fraud losses	Rise in client complaints

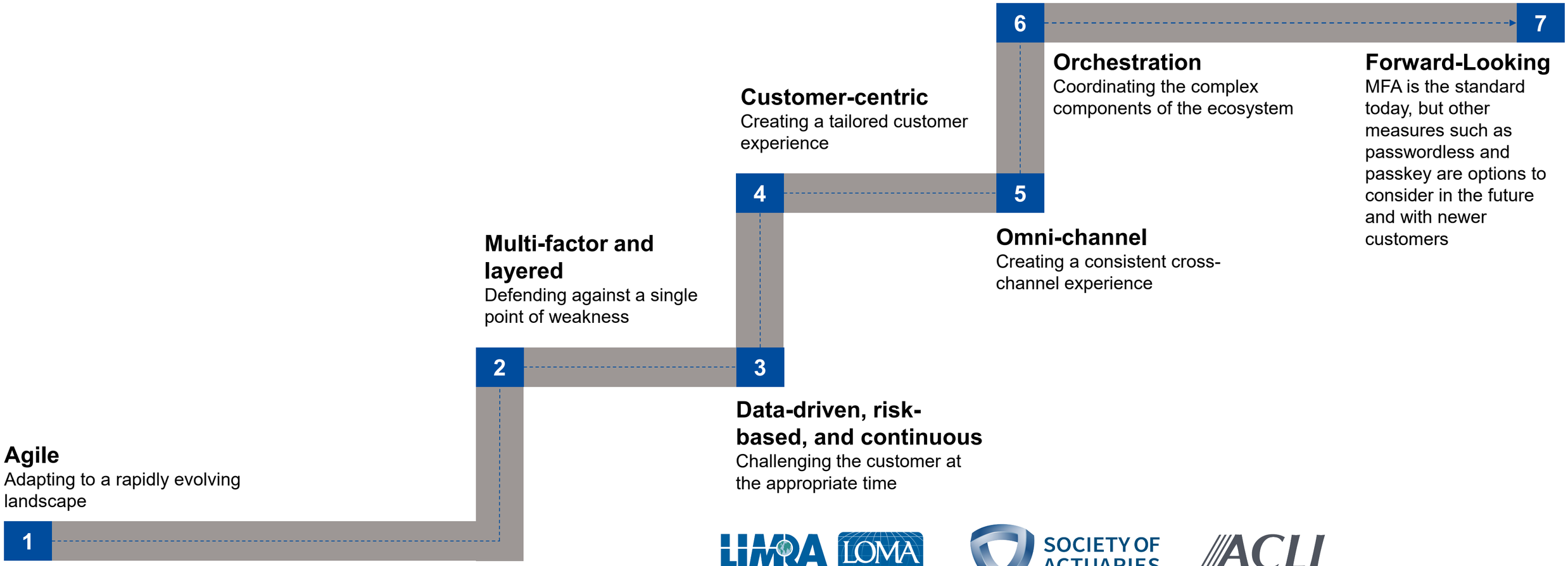
LIMRA LOMA Navigate With Confidence

SOCIETY OF ACTUARIES

ACLI Financial Security for Life

The roadmap to helping improve your future-state authentication

Traditional approaches of authentication (e.g., static knowledge-based authenticators) are lacking in the agility to adapt to the changing fraud landscape. The following design elements should be considered when designing next generation authentication strategies.



LIMRA LOMA
Navigate With Confidence

SOCIETY OF ACTUARIES

ACLI
Financial Security for Life

Multiple regulators are stepping up guidance advising firms to employ MFA

Insurance firms should continue to invest to meet the increasing regulatory scrutiny on authentication.

NYDFS Guidance on Multi-Factor Authentication[1]

NYDFS **scrutinized hundreds of cyber incidents for MFA not designed and implemented in a way to appropriately address risk**. Common weaknesses include MFA being absent, not fully implemented, or configured improperly.

FTC Step-Up Standards for MFA[2]

The FTC has expanded further proposals for the adoption of MFA, **requiring companies to use phishing-resistant MFA** for their employees.
It specifically rules out multi-factor solutions that use SMS, push notifications or one-time password.

CISA Publication on Phishing-Resistant MFA[3]

Not each form of MFA are equally secure. **Phishing-resistant MFA is the gold standard for MFA.** US Cybersecurity and Infrastructure Security Agency ("CISA") strongly urges system administrators and other high-value targets to plan their migration to phishing-resistant MFA.

Uniform Commercial Code and Commercially Reasonable Security Protocol[4]

Tokens and dual control security features may not be sufficient to conclude that a financial institution's security procedures are commercially reasonable.

Reference:

1. https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance
2. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems
3. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
4. https://www.law.cornell.edu/ucc/4a/article4a#:~:text=A%20security%20procedure%20is%20deemed,be%20bound%20by%20any%20payment

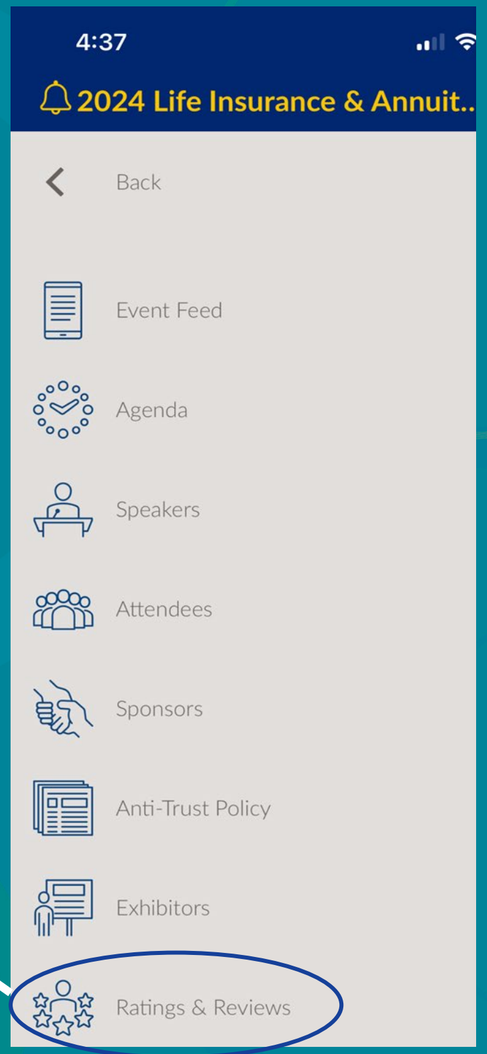
LIMRA LOMA Navigate With Confidence

SOCIETY OF ACTUARIES

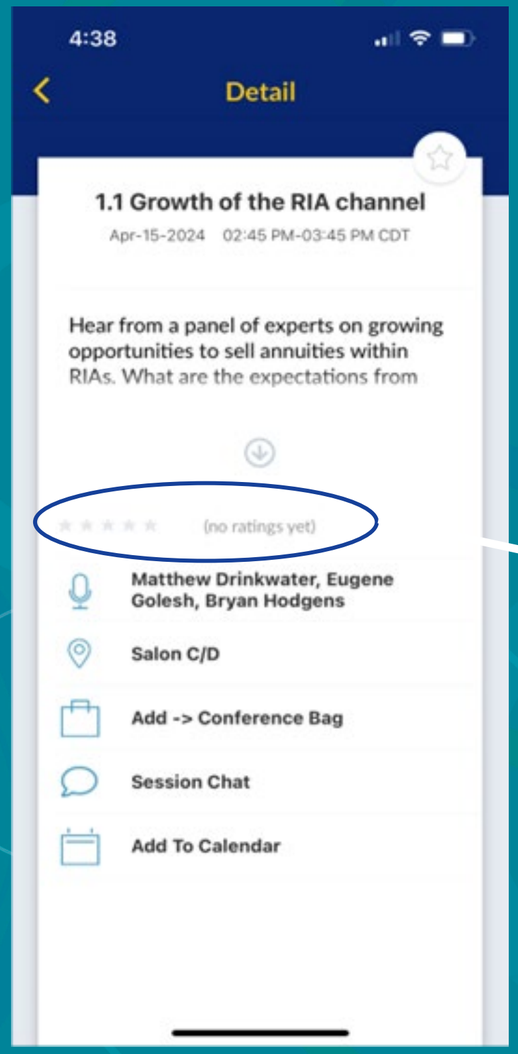
ACLI Financial Security for Life

Please Provide Your Feedback on the Conference App

OPTION 1



OPTION 2



LIMRA LOMA Navigate With Confidence

SOCIETY OF ACTUARIES®

ACLI Financial Security for Life

Thank You

LIMRA LOMA
Navigate With Confidence

SOCIETY OF ACTUARIES®

ACLI
Financial Security for Life