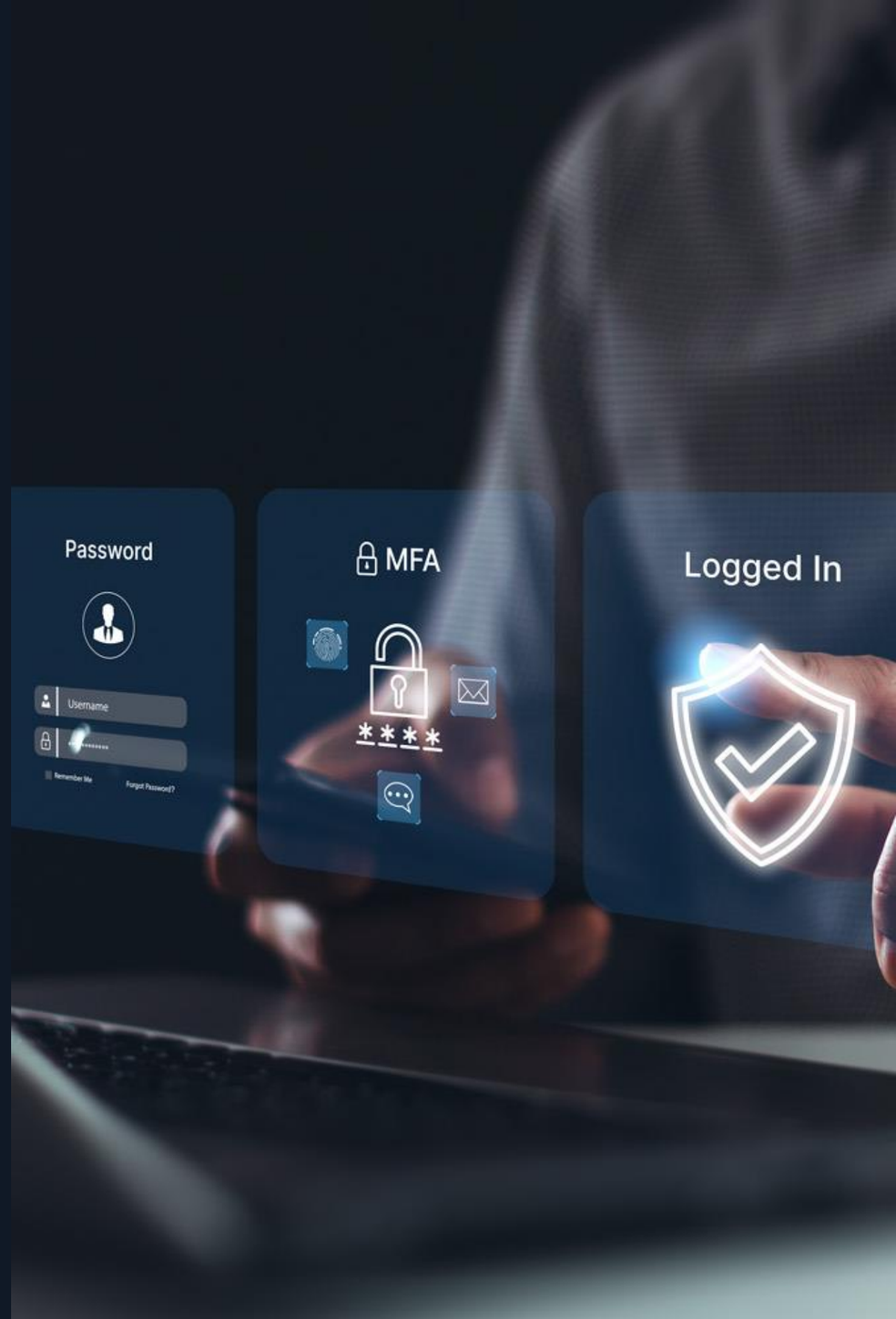
pillsbury Guidehouse outwit complexity™

FEBRUARY 6, 2025

How Safe Is Your Multi-Factor Authentication?

Complying with the NYDFS and Other Cybersecurity Regulators



Presented by:

Mark Krotoski | Pillsbury
Brian Montgomery | Pillsbury
Erik Pupo | Guidehouse

Presenters

Mark L. Krotoski

Partner & Cyber Disputes
Team Leader

Pillsbury

Brian H. Montgomery

Partner & Consumer Finance
Regulatory Team Leader

Pillsbury

Erik Pupo

Director, Commercial
Health IT Advisory

Guidehouse

pillsbury

Guidehouse
outwit complexity™

Preliminary Note

This presentation draws upon the experience of the presenters, discusses legal issues from varying perspectives, does **not** discuss or consider non-public case information in pending or past cases that they have been involved with, and does not necessarily reflect the views of our clients.

Agenda

- Overview of MFA, risks and vulnerabilities
- The role of MFA in cybersecurity in reducing cyber threats
- Lessons learned from recent incidents
- Regulatory requirements for MFA
- Using phishing-resistant MFA
- Best practices and recommendations

pillsbury Guidehouse outwit complexity™

Overview of MFA, Risks and Vulnerabilities

pillsbury

Guidehouse
outwit complexity™

Cybersecurity Risks and Vulnerabilities

- Key Premise
  - Threat actors target all security layers.
  - Threat actors recognize many companies use MFA.
  - Threat actors devise schemes to exploit and bypass MFA.
  - CISA: "[N]ot all forms of MFA are equally secure."

- We have assisted companies on cases where threat actors bypassed MFA.

pillsbury Guidehouse outwit complexity™

Exploiting MFA Gaps

"MFA weaknesses are the most common cybersecurity gap exploited at financial services companies. Since the [DFS] Cybersecurity Regulation went into effect, DFS has scrutinized hundreds of cyber incidents at DFS-licensed organizations ("Covered Entities"), and seen **MFA gaps exploited over and over again**. The **most common weaknesses … include MFA being absent, not fully implemented, or configured improperly**."

December 7, 2021

To: All Regulated Entities

Re: Guidance on Multi-Factor Authentication

Introduction

Multi-Factor Authentication ("MFA") is an essential part of cybersecurity hygiene. This was true even in 2016 and 2017, when the Department of Financial Services ("the Department" or "DFS") drafted 23 NYCRR Part 500 (the "Cybersecurity Regulation" or the "Regulation"). MFA was already considered an essential control, which is why it was one of the few technical controls explicitly required by the Regulation.[1] MFA's importance hasn't changed – if anything, the increase in cybercrime has made MFA even more essential.

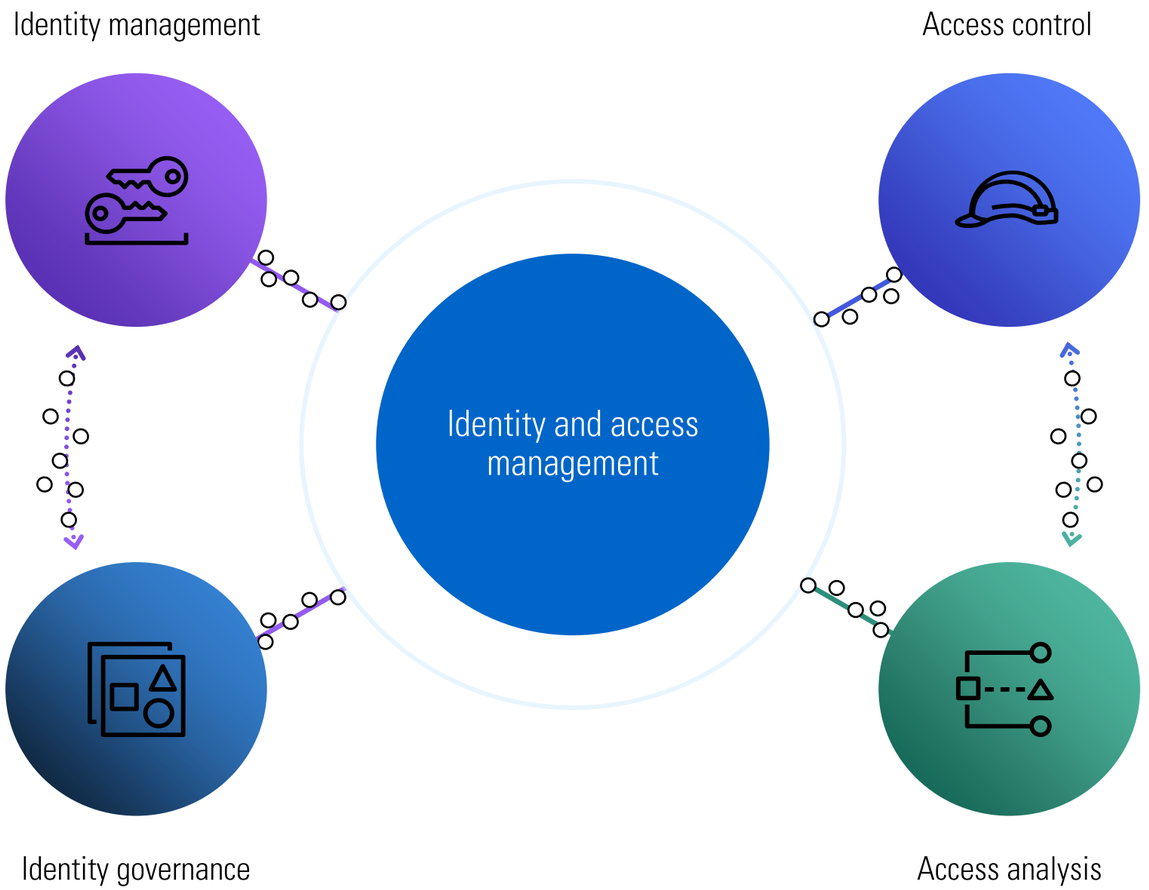
MFA weaknesses are the most common cybersecurity gap exploited at financial services companies. Since the Cybersecurity Regulation went into effect, DFS has scrutinized hundreds of cyber incidents at DFS-licensed organizations ("Covered Entities"),[2] and seen MFA gaps exploited over and over again. The most common weaknesses are described below and include MFA being absent, not fully implemented, or configured improperly.

MFA failures have real consequences for financial services companies and consumers. In fact, from January 2020 to July 2021, DFS found that more than 18.3 million consumers were impacted by cyber incidents reported to DFS pursuant to Section 500.17(a) ("Cybersecurity Events")[3] in which Covered Entities had MFA failures. Over 870 thousand of those consumers were New Yorkers.

MFA is therefore a focus of DFS's cybersecurity supervisory and enforcement work. As part of this focus, DFS has resolved two enforcement actions in the past year against companies that were required to implement MFA but had not fully done so and that failed to prevent unauthorized access to their nonpublic information.[4] DFS is also increasing its review of MFA during examinations, with a particular emphasis on probing for the common MFA failures discussed in this Guidance.

Source: Industry Letter - December 7, 2021: Guidance on Multi-Factor Authentication | Department of Financial Services

Enforce Strong Security Access Controls



pillsbury

Guidehouse
outwit complexity™

Why Security Access Controls?

Grant the right access, to the right people, at the right time

Use multi-factor authentication (MFA)

Use federation with centralized IDP

Require workloads to use temporary credentials

Set up policy validation

Builds on IAM roles and policies to help manage access centrally

Balancing least privilege with business needs, apply fine-grained permissions with conditions

Establishing a data perimeter and permissions guardrails

Review and audit access regularly

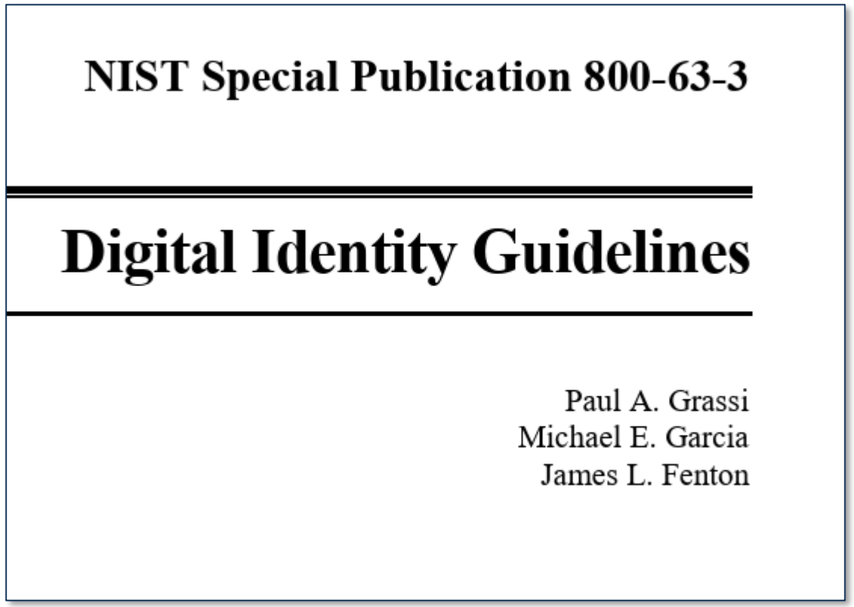
pillsbury

Guidehouse outwit complexity™

What Is Multi-Factor Authentication (MFA)?

National Institute of Standards and Technology Definition

- "Multi-Factor Authentication (MFA) An authentication system that requires more than one distinct authentication factor for successful authentication."
- "Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors."
- "The three authentication factors are:
  - **something you know,**
  - **something you have, and**
  - **something you are.**"


NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

pillsbury Guidehouse outwit complexity™

Source: NIST Special Publication 800-63-3 Digital Identity Guidelines

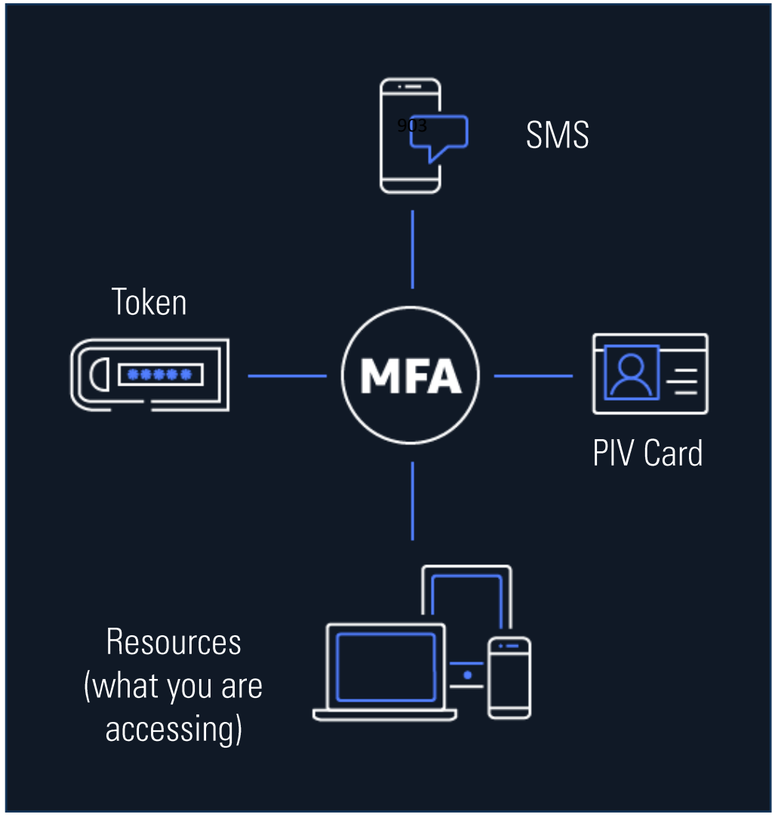
What Is Multi-Factor Authentication (MFA)?

MFA adds an extra layer of protection on top of name and password for root, interactive IAM users.

- Virtual MFA devices
- U2F security key
- Hardware MFA device
- SMS text message-based MFA

Identity federation changes the approach, but it is not a best practice.

- Use MFA at your identity provider.



Types of Physical MFA

Multi-factor authentication (MFA)

- Helps prevent anyone with unauthorized knowledge of your credentials from impersonating you.
- Virtual, hardware, U2F
- Works with:
  - Root credentials
  - Users
  - Applications
- Integrated into:
  - APIs
  - Applications
  - Key pages
  - Requirement for access to files and folders

pillsbury Guidehouse outwit complexity™

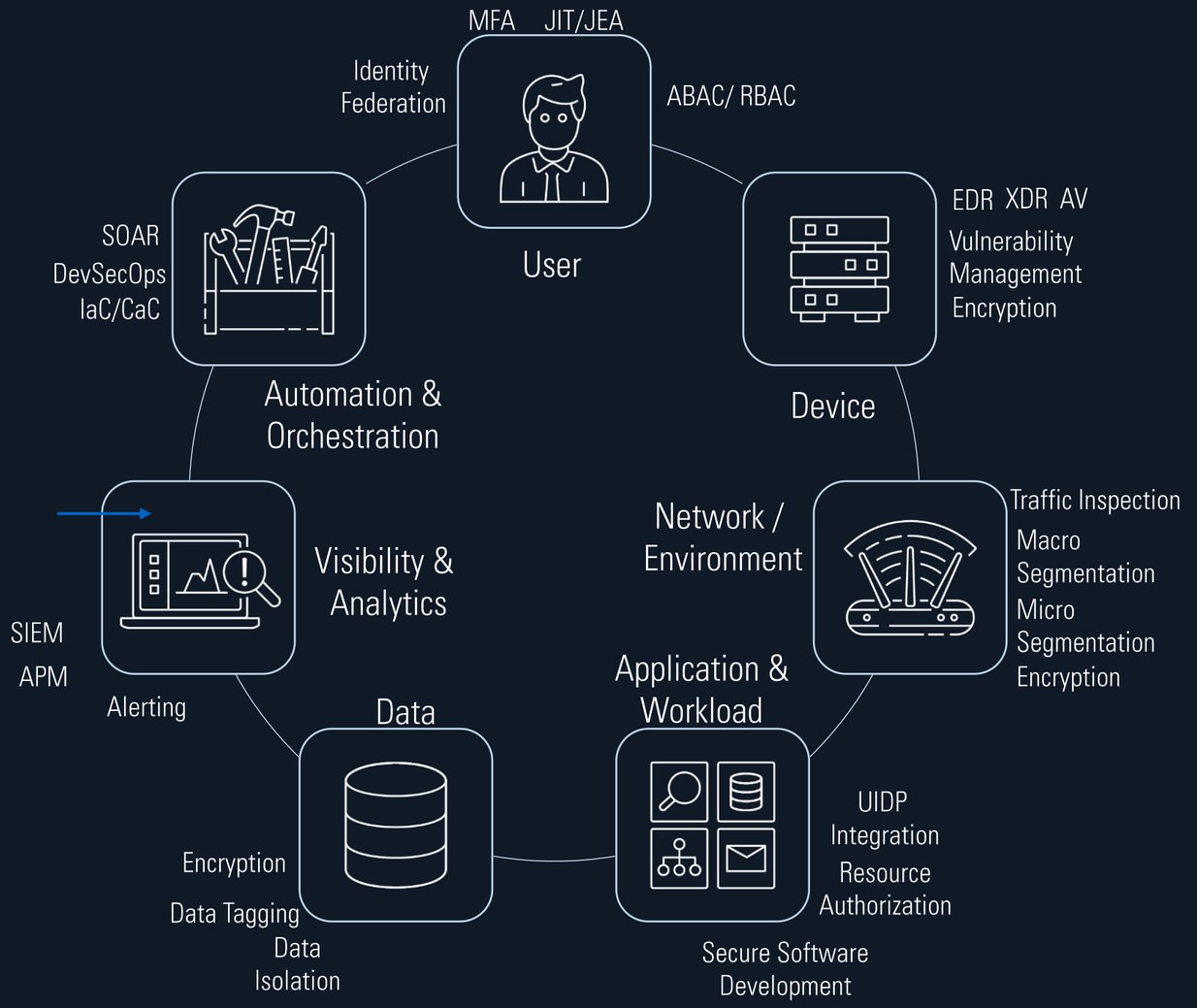
What Is a Zero Trust model?

A conceptual **security model** and associated set of **mechanisms** that focus on providing security controls around digital assets that **do not solely or fundamentally depend** on traditional network controls or network perimeters

Adopt Zero Trust Model

Enterprise Managed
Identity + MFA

Continuous
Verification



pillsbury

Guidehouse
outwit complexity™

How Does MFA Apply?

Target

- Multi-Factor Authentication (MFA)
- User & Application Inventory
- Least-Privilege Access
- Macro-Segmentation
- Unified Endpoint Management & Mobile Device Management (UEM/MDM)
- Encryption
- Vulnerability Management
- Security and Audit Logging

Target → Advanced

- Federation Based on Enterprise Identity
- Fine-Grained User and Device Access
- Micro-Segmentation
- Baseline User and Entity Behavior Analytics (UEBA)
- Endpoint Detection (AV, FIM, HIPS/HIDS, App Control)
- Critical Process Automation (IaC)
- Automated Vulnerability and Patch Management

Advanced

- Real-Time Dynamic Access to Data, Applications, Assets and Services (DAAS)
- Continuous Authentication and Authorization (JIT/JEA)
- Advanced Analytics Enable Automated and Orchestrated Threat Response (SOAR)
- AI/ML Baseline Activity Monitoring and Response
- Endpoint Automated Response (XDR)
- Data Loss Prevention (DLP) Program in Place with Data Tagging

pillsbury Guidehouse outwit complexity™

The Role of MFA in Cybersecurity in Reducing Cyber Threats

pillsbury

Guidehouse
outwit complexity™

Common MFA Exploits

- Authenticator codes
- Short message service (SMS) codes
  - One-time passwords (OTP) or SMS codes
  - Tricking users into providing their codes
- “Push bombing” attacks
- SIM swap attacks
- Social engineering
- Exploitation of Signaling System 7 (SS7) protocol vulnerabilities

pillsbury Guidehouse outwit complexity™

Source: Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA’s Fast IDentity Online (FIDO) Implementation | CISA; CISA Implementing Phishing-Resistant MFA Fact Sheet - October 2022

Why Is MFA Important?

- “Implementing MFA makes it more difficult for a threat actor to gain access to business premises and information systems, such as remote access technology, email, and billing systems, even if passwords or PINs are compromised through phishing attacks or other means.”
- “Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. **MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries**.”

MULTI-FACTOR AUTHENTICATION

JANUARY 2022

OVERVIEW

Multi-factor authentication (MFA) is a layered approach to securing physical and logical access where a system requires a user to present a combination of two or more different authenticators to verify a user's identity for login. MFA increases security because even if one authenticator becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space or computer system.

WHY IS MFA IMPORTANT?

Implementing MFA makes it more difficult for a threat actor to gain access to business premises and information systems, such as remote access technology, email, and billing systems, even if passwords or PINs are compromised through phishing attacks or other means.

Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.

HOW DOES MFA WORK?

MFA requires users to present two or more authentication factors at login to verify their identity before they are granted access. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- Something you know: like a password or Personal Identification Number (PIN);
- Something you have: like a smart card, mobile token, or hardware token; and,
- Some form of biometric factor (e.g., fingerprint, palm print, or voice recognition).

For example, MFA could require users to insert a smart card or a bank card into a card reader (first factor) and then enter a password or a PIN (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

Consider enforcing MFA on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs). Implementation schedules, costs, adoption willingness, and the degree of protection provided vary depending on the solutions selected and the platforms to be protected, so match the capability to the need.

If you have questions or suggestions regarding this product, please feel free to contact CISA Central at mailto:central@cisa.govand reference the Multi-factor Authentication document in the subject line.

Source: CISA Multi-Factor Authentification Fact Sheet - January 2022

Why Is MFA Important?

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

- "The use of MFA on your accounts makes you **99% less likely to be hacked**."
- "MFA is a **layered approach** to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login."
- "MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database."

pillsbury Guidehouse outwit complexity™

Source: Multifactor Authentication | Cybersecurity and Infrastructure Security Agency CISA

Lessons Learned from Recent Incidents

pillsbury

Guidehouse
outwit complexity™

NYDFS Secures $2 Million Cybersecurity Settlement with PayPal, Inc. (Jan. 23, 2025)

"Notably, the company did not require customers to use multifactor authentication or use controls such as CAPTCHA or rate limiting to help prevent unauthorized access. PayPal has since remediated these issues and improved its cybersecurity practices."

Source: Superintendent Adrienne A. Harris Secures $2 Million Cybersecurity Settlement with PayPal, Inc.; In the Matter of PAYPAL, INC. Consent Order

HHS Office for Civil Rights Imposes a $548,265 Penalty Against Children's Hospital for HIPAA Privacy and Security Rules Violations

- "OCR's investigation determined that the first reported breach occurred **because multi-factor authentication was disabled** on an email account."
- "OCR recommends that health care providers, health plans, health care clearinghouses, and business associates that are covered by HIPAA take the following steps to mitigate or prevent cyber-threats:
  - Utilize multi-factor authentication to ensure only authorized users are accessing ePHI."

HHS Office for Civil Rights Imposes a $548,265 Penalty Against Children's Hospital Colorado for HIPAA Privacy and Security Rules Violations

Multiple HIPAA violations lead to OCR's 7th penalty of the year.

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a $548,265 civil monetary penalty against Children's Hospital Colorado, concerning violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules following receipt of breach reports in 2017 and 2020, relating to email phishing and cyberattacks . OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules, which set forth the requirements that covered entities (health plans, health care clearinghouses, and most health care providers), and business associates must follow to protect the privacy and security of protected health information (PHI). The HIPAA Security Rule establishes national standards to protect and secure our health care system by requiring administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI (ePHI).

"Email continues to be a very common way for cyberattackers to enter health information systems and jeopardized privacy and security," said OCR Director Melanie Fontes Rainer. "Health care entities should identify potential risks and vulnerabilities to email accounts and train their workforce to protect health information in those accounts."

OCR investigated Children's Hospital Colorado following breaches which reported a phishing attack that compromised an email account containing 3,370 individuals' PHI and another after three email accounts were breached, containing 10,840 individuals' PHI. OCR's investigation determined that the first reported breach occurred because multi-factor authentication was disabled on an email account. The second breaches occurred, in part, when workforce members gave permission to unknown third parties to access their email accounts. OCR also found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems.

pillsbury Guidehouse outwit complexity™

Source: 2025-01-02 05:49 | Archive of HHS.gov

SEC: *In the Matter of Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc.* (Feb. 9, 2024)

"Although Cambridge discovered the first email account takeover in January 2018, it failed to adopt and implement firm wide enhanced security measures for cloud-based email accounts of its independent representatives in its written policies and procedures, **such as the use of multi-factor authentication ("MFA")**, for all Cambridge users until 2021. This resulted in the exposure of sensitive customer records and information, including PII, of Cambridge customers and the potential exposure of additional customer records and information."

Source: https://www.sec.gov/files/litigation/admin/2021/34-92806.pdf

SEC: *In the Matter of Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC.*

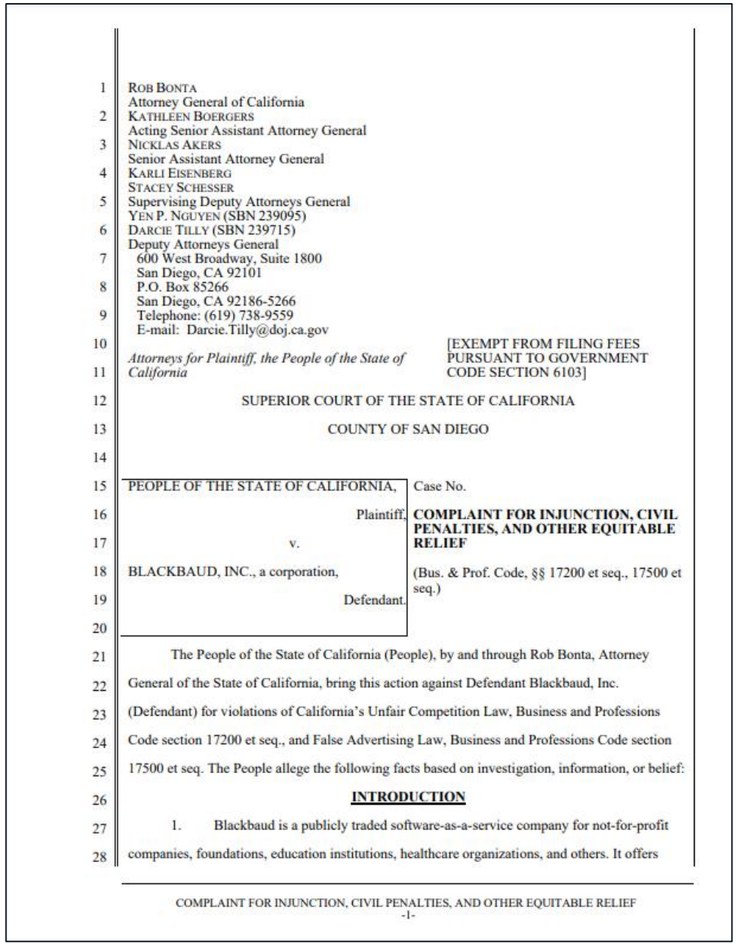
"Between November 2017 and June 2020, email accounts of over 60 Cetera Entities' personnel were taken over by unauthorized third parties resulting in the exposure of over 4,388 of Cetera Entities' customers' personally identifiable information ("PII") stored in the compromised email accounts. At the time, **none of these accounts had multi-factor authentication ("MFA") turned on**, even though Cetera Entities' own policies required MFA "wherever possible," beginning in 2018."

pillsbury Guidehouse outwit complexity™

Source: https://www.sec.gov/files/litigation/admin/2021/34-92800.pdf

California Attorney General Secures $6.75 Million Settlement Against Blackbaud over 2020 Data Breach

"The California Department of Justice's investigation revealed that Blackbaud failed to carry out basic security procedures that would have fixed known technological vulnerabilities **such as implementing multi-factor authentication for passwords** and did not properly monitor suspicious activity occurring on systems that maintained personal information. "



ROB BONTA
Attorney General of California
KATHLEEN BOERGERS
Acting Senior Assistant Attorney General
NICKLAS AKERS
Senior Assistant Attorney General
KARLI EISENBERG
STACEY SCHESSER
Supervising Deputy Attorneys General
YEN P. NGUYEN (SBN 239095)
DARCIE TILLY (SBN 239715)
Deputy Attorneys General
600 West Broadway, Suite 1800
San Diego, CA 92101
P.O. Box 85266
San Diego, CA 92186-5266
Telephone: (619) 738-9559
E-mail: Darcie.Tilly@doj.ca.gov

Attorneys for Plaintiff, the People of the State of California

[EXEMPT FROM FILING FEES PURSUANT TO GOVERNMENT CODE SECTION 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff,
v.
BLACKBAUD, INC., a corporation,
Defendant.

Case No.

COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF

(Bus. & Prof. Code, §§ 17200 et seq., 17500 et seq.)

The People of the State of California (People), by and through Rob Bonta, Attorney General of the State of California, bring this action against Defendant Blackbaud, Inc. (Defendant) for violations of California's Unfair Competition Law, Business and Professions Code section 17200 et seq., and False Advertising Law, Business and Professions Code section 17500 et seq. The People allege the following facts based on investigation, information, or belief:

INTRODUCTION

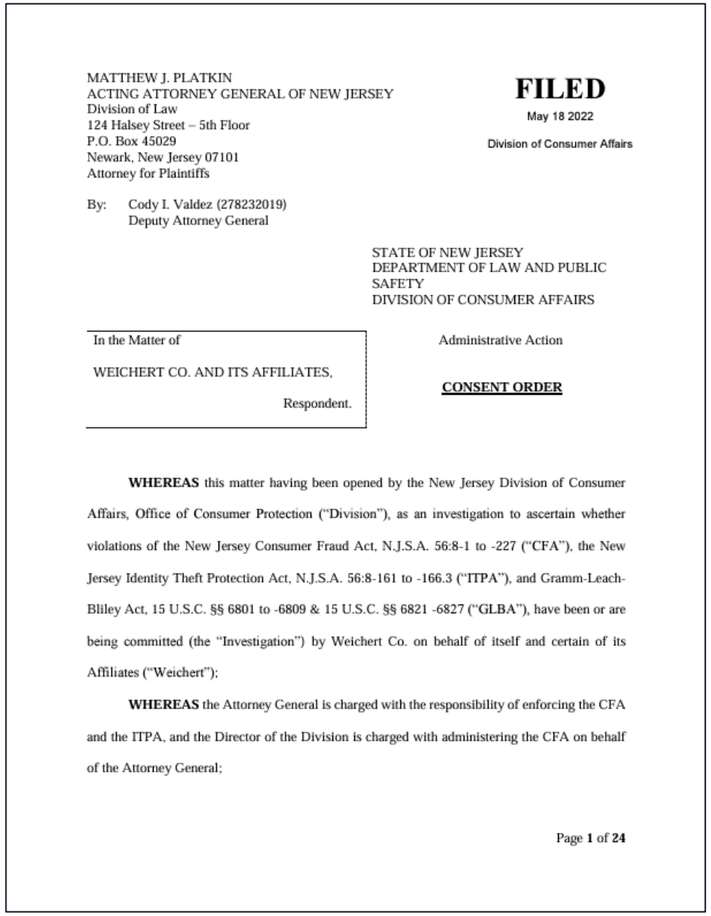
1. Blackbaud is a publicly traded software-as-a-service company for not-for-profit companies, foundations, education institutions, healthcare organizations, and others. It offers

COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF
-1-

Source: Attorney General Bonta Secures $6.75 Million Settlement Against Blackbaud Over 2020 Data Breach | State of California - Department of Justice - Office of the Attorney General; People of the State of California v. Blackbaud, Inc. | Complaint

New Jersey AG Settlement with Real Estate and Financial Group over Data Breach and Inadequate Cybersecurity Measures (May 18, 2022)

"Based on its investigation, the Division alleges that among other things, Weichert misrepresented security practices to consumers, lacked antivirus software to protect its network, and **failed to implement multi-factor authentication that would have prevented unauthorized access**."



MATTHEW J. PLATKIN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street – 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for Plaintiffs

By: Cody I. Valdez (278232019)
Deputy Attorney General

FILED
May 18 2022
Division of Consumer Affairs

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC SAFETY
DIVISION OF CONSUMER AFFAIRS

In the Matter of
WEICHERT CO. AND ITS AFFILIATES,
Respondent.

Administrative Action

CONSENT ORDER

WHEREAS this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection ("Division"), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -227 ("CFA"), the New Jersey Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166.3 ("ITPA"), and Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 to -6809 & 15 U.S.C. §§ 6821 -6827 ("GLBA"), have been or are being committed (the "Investigation") by Weichert Co. on behalf of itself and certain of its Affiliates ("Weichert");

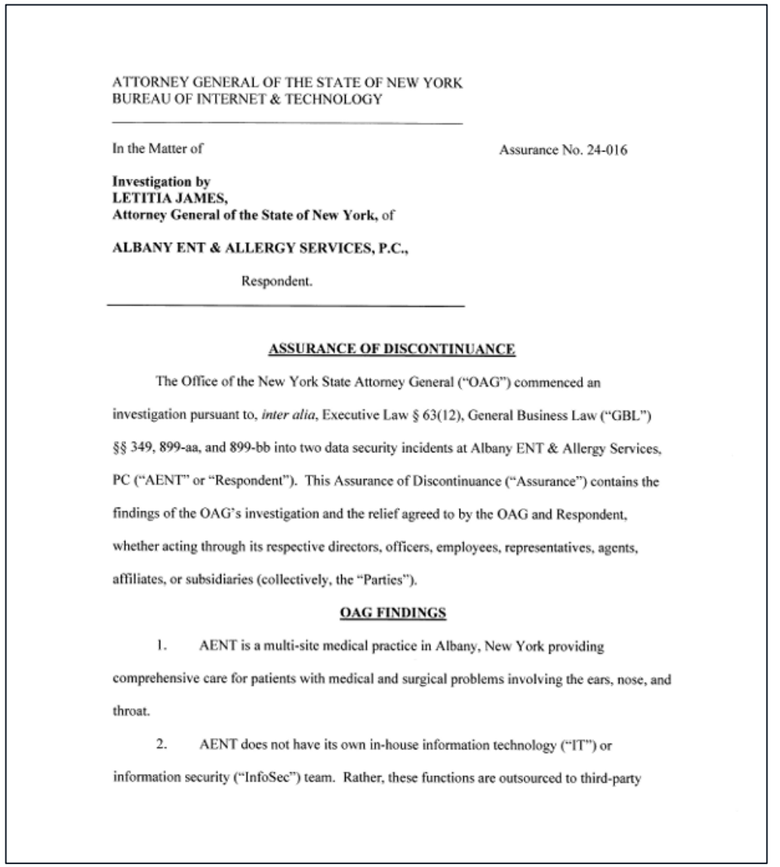
WHEREAS the Attorney General is charged with the responsibility of enforcing the CFA and the ITPA, and the Director of the Division is charged with administering the CFA on behalf of the Attorney General;

Page **1** of **24**

Source: Acting AG Platkin Reaches Settlement with Real Estate and Financial Group over Data Breach and Inadequate Cybersecurity Measures - New Jersey Office of Attorney General; In the Matter of WEICHERT CO. AND ITS AFFILIATES | Consent Order

NY Attorney General Secures $2.25 Million from Capital Region Health Care Provider to Protect Patient Data

"[V]endors did not timely install critical security software updates, adequately log and monitor network activity, properly encrypt consumers' private information before and after the attacks, **utilize multi-factor authentication for all remote access**, or otherwise maintain a reasonable information security program."



ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of — Assurance No. 24-016

Investigation by
LETITIA JAMES,
Attorney General of the State of New York, of

ALBANY ENT & ALLERGY SERVICES, P.C.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the New York State Attorney General ("OAG") commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12), General Business Law ("GBL") §§ 349, 899-aa, and 899-bb into two data security incidents at Albany ENT & Allergy Services, PC ("AENT" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and Respondent, whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").

OAG FINDINGS

1. AENT is a multi-site medical practice in Albany, New York providing comprehensive care for patients with medical and surgical problems involving the ears, nose, and throat.

2. AENT does not have its own in-house information technology ("IT") or information security ("InfoSec") team. Rather, these functions are outsourced to third-party

Source: Attorney General James Secures $2.25 Million from Capital Region Health Care Provider to Protect Patient Data ; In the Matter of Investigation by Letitia James, Attorney General of the State of New York, of ALBANY ENT & ALLERGY SERVICES, P.C. | Assurance of Discontinuance

Regulatory Requirements for MFA

pillsbury

Guidehouse
outwit complexity™

Executive Order (Oct. 17, 2014)

"Sec. 3. Securing Federal Transactions Online. To help ensure that sensitive data are shared only with the appropriate person or people, within 90 days of the date of this order, the National Security Council staff, the Office of Science and Technology Policy, and OMB shall present to the President a plan, consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace, to ensure that all agencies making personal data accessible to citizens through digital applications **require the use of multiple factors of authentication and an effective identity proofing process**, as appropriate. Within 18 months of the date of this order, relevant agencies shall complete any required implementation steps set forth in the plan prepared pursuant to this section.."

For Immediate Release October 17, 2014

Executive Order --Improving the Security of Consumer Financial Transactions

pillsbury Guidehouse outwit complexity™

Source: Executive Order --Improving the Security of Consumer Financial Transactions | whitehouse.gov

Improving the Nation's Cybersecurity
Executive Order 14028 (May 12, 2021)

"(d) Within 180 days of the date of this order, **agencies shall adopt multi-factor authentication and encryption for data at rest and in transit**, to the maximum extent consistent with Federal records laws and other applicable laws."

"(i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multifactor authentication and encryption of data at rest and in transit. Such agencies shall provide such **reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption**."

Source: Federal Register :: Improving the Nation's Cybersecurity

NYDFS Cybersecurity Regulation Requirement

Section 500.12 Multi-Factor Authentication

- (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include **Multi-Factor Authentication or Risk-Based Authentication**, to protect against unauthorized access to Nonpublic Information or Information Systems.
- (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Reasonably Equivalent or More Secure Access Controls

Section 500.12 Multi-Factor Authentication

- NYDFS conducts regular cybersecurity examinations of Covered Entities.

- If a Covered Entity's CISO has approved an alternative to MFA, examiners will likely closely scrutinize this choice, and Covered Entities should be prepared to support this position.

NYDFS Annual Certification of Material Compliance or Acknowledgement of Noncompliance

Section 500.17(b)(1)

- By **April 15**, for prior calendar year
- Signed by the **highest-ranking executive** and the **CISO**
- Maintain records “for examination and inspection by” DFS “for a period of five years”

Using Phishing-Resistant MFA

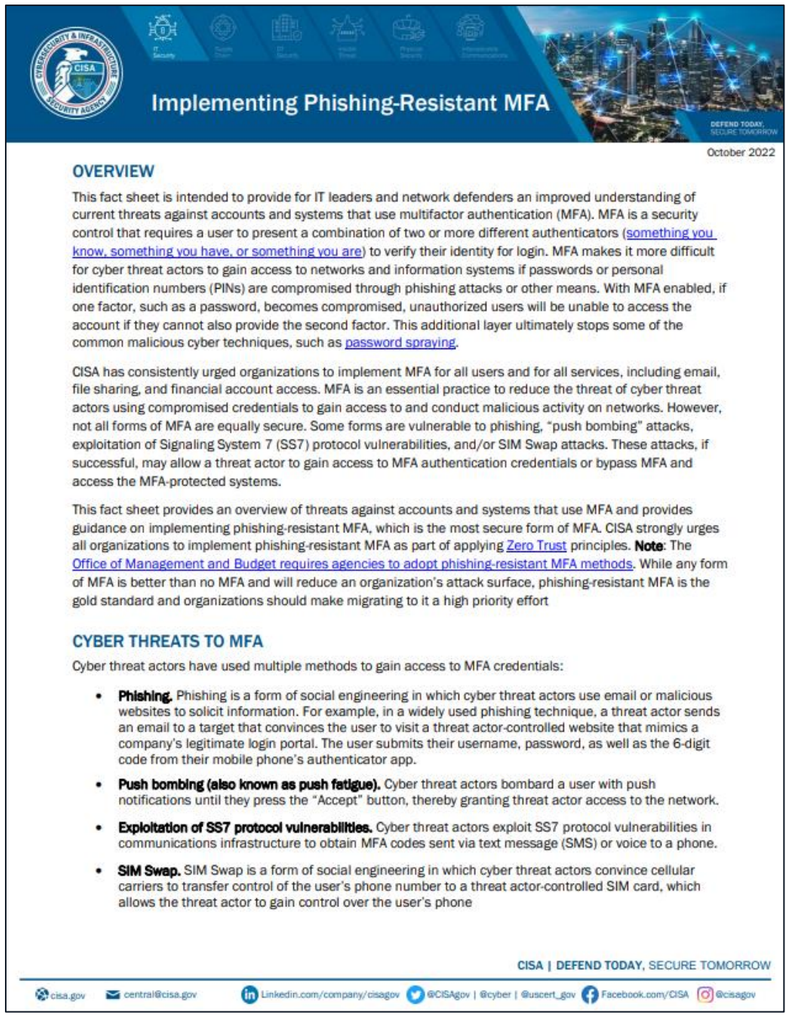
pillsbury

Guidehouse
outwit complexity™

CISA: Implementing Phishing-Resistant MFA

"CISA has consistently urged organizations to implement MFA for all users and for all services, including email, file sharing, and financial account access. MFA is an essential practice to reduce the threat of cyber threat actors using compromised credentials to gain access to and conduct malicious activity on networks. However, not all forms of MFA are equally secure."

"While any form of MFA is better than no MFA and will reduce an organization's attack surface, **phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort**."



Implementing Phishing-Resistant MFA

October 2022

OVERVIEW

This fact sheet is intended to provide for IT leaders and network defenders an improved understanding of current threats against accounts and systems that use multifactor authentication (MFA). MFA is a security control that requires a user to present a combination of two or more different authenticators (something you know, something you have, or something you are) to verify their identity for login. MFA makes it more difficult for cyber threat actors to gain access to networks and information systems if passwords or personal identification numbers (PINs) are compromised through phishing attacks or other means. With MFA enabled, if one factor, such as a password, becomes compromised, unauthorized users will be unable to access the account if they cannot also provide the second factor. This additional layer ultimately stops some of the common malicious cyber techniques, such as password spraying.

CISA has consistently urged organizations to implement MFA for all users and for all services, including email, file sharing, and financial account access. MFA is an essential practice to reduce the threat of cyber threat actors using compromised credentials to gain access to and conduct malicious activity on networks. However, not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems.

This fact sheet provides an overview of threats against accounts and systems that use MFA and provides guidance on implementing phishing-resistant MFA, which is the most secure form of MFA. CISA strongly urges all organizations to implement phishing-resistant MFA as part of applying Zero Trust principles. **Note**: The Office of Management and Budget requires agencies to adopt phishing-resistant MFA methods. While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort

CYBER THREATS TO MFA

Cyber threat actors have used multiple methods to gain access to MFA credentials:

- **Phishing.** Phishing is a form of social engineering in which cyber threat actors use email or malicious websites to solicit information. For example, in a widely used phishing technique, a threat actor sends an email to a target that convinces the user to visit a threat actor-controlled website that mimics a company's legitimate login portal. The user submits their username, password, as well as the 6-digit code from their mobile phone's authenticator app.
- **Push bombing (also known as push fatigue).** Cyber threat actors bombard a user with push notifications until they press the "Accept" button, thereby granting threat actor access to the network.
- **Exploitation of SS7 protocol vulnerabilities.** Cyber threat actors exploit SS7 protocol vulnerabilities in communications infrastructure to obtain MFA codes sent via text message (SMS) or voice to a phone.
- **SIM Swap.** SIM Swap is a form of social engineering in which cyber threat actors convince cellular carriers to transfer control of the user's phone number to a threat actor-controlled SIM card, which allows the threat actor to gain control over the user's phone

CISA | DEFEND TODAY, SECURE TOMORROW

cisa.gov central@cisa.gov Linkedin.com/company/cisagov @CISAgov | @cyber | @uscert_gov Facebook.com/CISA @cisagov

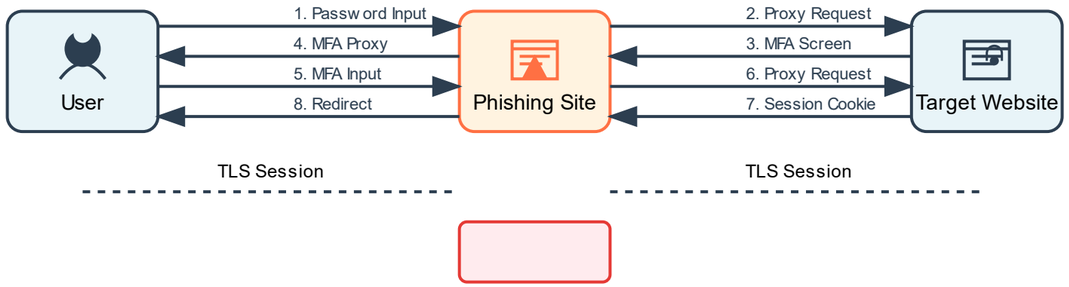
pillsbury Guidehouse outwit complexity™

Source: Implementing Phishing-Resistant MFA

What Is a Phishing MFA Attack?

MFA is the best way to protect resources from inappropriate access. Always set up MFA on your root user and all users.

However, phishing attacks can defeat MFA if they convince a user to share a password with a website.



Understanding Phishing-Resistant MFA

- Phishing-resistant MFA enhances security by using unique codes. Phishing-resistant MFA enhances security for health care data.
- Utilizes biometric authentication for patient access. Requires physical devices for secure transactions.
- Protects sensitive health information from unauthorized access. It requires user interaction and physical devices for authentication. This method protects sensitive information from phishing attacks.

pillsbury Guidehouse outwit complexity™

Benefits of Phishing-Resistant MFA

- Decreases risk of unauthorized access to accounts
- Enhances trust in online transactions and communications
- Promotes compliance with security regulations

pillsbury Guidehouse outwit complexity™

Best Practices and Recommendations

pillsbury

Guidehouse
outwit complexity™

Core Best Practices for Phishing-Resistant MFA

Adopt FIDO2/WebAuthn Authentication

- Require cryptographic proof from physical device
- Local verification on authenticator
- Multiple token registration per user
- Silent authentication for reduced friction

Use Hardware Security Keys

- FIDO-certified with tamper-evident features
- NFC capability for mobile authentication
- Secure key provisioning process
- Emergency access procedures

Use Certificate-Based Authentication

- Internal certificate authority deployment
- Real-time certificate validation
- Certificate pinning implementation
- Automated life cycle management

How to Sustain Phishing-Resistant MFA

Policy Controls

- Risk-based adaptive authentication
- Geolocation access controls
- Device health verification
- Dynamic session management

Technical Integration into Your Security Architecture

- Directory service synchronization
- SSO implementation (SAML 2.0/OAuth 2.0)
- API security measures
- Mobile device considerations

Continuous Monitoring of MFA components

- Real-time authentication tracking
- Automated response procedures
- Regular security assessments
- Compliance auditing processes

pillsbury Guidehouse outwit complexity™

NYDFS Exams and Compliance Certifications

- Covered entities should be prepared to defend any decision to implement a “reasonable alternative” to MFA.

- Covered entities must submit annual certifications of compliance (or noncompliance) and should carefully consider those certifications (which must be signed by senior officials) and the process to arrive at certification.

Best Practices and Recommendations

- Recall Key Premise
  - Threat actors target all security layers.
  - Threat actors recognize many companies use MFA.
  - Threat actors devise schemes to exploit and bypass MFA.
  - CISA: "[N]ot all forms of MFA are equally secure."
- MFA offers one important security layer for access controls.
- Consider security holistically along with other security layers.

pillsbury Guidehouse outwit complexity™

Questions

pillsbury

Guidehouse
outwit complexity™

Mark L. Krotoski

Partner, Litigation
Pillsbury
Full Biography
+1.650.233.4021
mark.krotoski@pillsburylaw.com

Litigation partner, leads Cyber Disputes team and Cartel Enforcement team, with more than 25 years' experience handling cybersecurity cases, investigations and issues.

Mark assists clients on cyber litigation and disputes, responding to a data breach, cyber incident or misappropriation of trade secrets, conducting confidential cybersecurity investigations, mitigating and remediating cyber risks, developing cybersecurity protection plans, responding to regulatory investigations, and coordinating with law enforcement on cyber crime issues.

At DOJ, he prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, trade secret and criminal intellectual property cases.

Mark served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cyber crime prosecutor in Silicon Valley, among other DOJ leadership positions.

Representative Experience

- Represented companies in complying with standards under the New York Department of Financial Services Cybersecurity Regulation.
- In representing an international retail company, led the forensic investigation concerning a cyberattack involving the acquisition of millions of customer records in all U.S. jurisdictions and more than 100 countries, provided guidance on legal obligations and coordinated with law enforcement, resulting in the identification and conviction of the perpetrator outside the United States.
- Represents clients on cyberattacks and violations of the Computer Fraud and Abuse Act including data breach class action cases.
- In the Yahoo data breach involving "at least 500 million" stolen user accounts, represented the manager of incident response during all phases of the investigation by the Department of Justice, Securities and Exchange Commission and Special Committee.
- Represented numerous companies in responding to ransomware and other cyberattacks, including through all phases involving the internal forensic investigation under attorney client privilege, review of data to determine notification requirements, notifications to federal and state regulators, responding to federal and state regulatory investigations, and follow-on litigation.
- Represented numerous international and domestic companies during investigations of cyber fraud and unauthorized wire transfers (referred to as a "business email compromise").
- Represented multiple companies in cyber risk assessments during an acquisition of or merger with another company.
- Lead counsel in a jury trial resulting in the conviction related to the intrusion into the Yahoo account of Alaska Governor Sarah Palin and obstruction of justice. Successfully argued the appeal before the U.S. Court of Appeals for the Sixth Circuit, affirming conviction.
- Lead counsel in a jury trial conviction of a system administrator who planted a "time bomb" on the company network after his departure.

Brian H. Montgomery

Senior Counsel, Financial Industry Group
Pillsbury
Full Biography
+1.212.858.1238
brian.montgomery@pillsburylaw.com

Brian Montgomery utilizes his background in consumer protection and financial services regulation to strategically advise businesses on state and federal regulatory compliance.

Brian's practice focuses on representing and advising banks, non-bank financial institutions, fintech companies, money services businesses and other businesses on regulatory and compliance matters, with a particular focus on consumer financial products and services. He regularly advises companies on how to navigate regulatory issues as they bring innovative financial products and services to market. Brian also counsels clients on compliance with regulators' cybersecurity, information technology and third-party risk management requirements.

Prior to joining the firm, Brian served in several senior positions at the New York Department of Financial Services, including leading the department's program to examine regulated institutions for compliance with federal and state consumer financial laws. Brian also supervised a group that conducted investigations and brought enforcement actions involving consumer financial products and services.

Representative Experience

- Advising financial institutions on U.S. financial services regulators' cybersecurity regulations and guidance.
- Supervised investigation of a significant data breach at a financial institution, resulting in a consent order.
- Representing several commercial banks in developing and roll-out of nationwide digital banking platforms, including regulatory and related issues.
- As deputy superintendent at the New York Department of Financial Services, oversaw consumer compliance and fair lending examinations of banks, non-depository lenders, loan servicers, credit reporting agencies and other regulated institutions, as well as Community Reinvestment Act examinations.
- Advising several consumer and commercial lenders on regulatory requirements for lending programs, including startup and ongoing compliance.
- Advising banks on compliance with Office of the Comptroller of the Currency (OCC) and Federal Financial Institutions Examination Council (FFIEC) requirements for third-party risk management and technology service providers.
- Provided guidance, in conjunction with Tokyo-based law firm, City-Yuwa, to the Japanese Financial Services Agency (FSA) regarding how to appropriately regulate the trading of stablecoins, a digital currency attached to a stable reserve asset, in Japan under the country's amended Payment Services Act.
- Served on the Virtual Currency Licensing Committee at the New York Department of Financial Services.
- Brought first action by state banking regulator under Title X of Dodd-Frank, the Consumer Financial Protection Act, resulting in consent judgment with auto lender and its president.
- Core member of the team that drafted the New York Financial Services Law and associated legislation that created the NYDFS by merging the banking and insurance departments. Subsequently planned and coordinated the merger of the consumer protection functions of the former departments.

Erik Pupo

Director, Commercial Health IT Advisory
Guidehouse
LinkedIn
+1.954.226.0974
epupo@guidehouse.com

Guidehouse
outwit complexity™

Erik is a Senior Executive in Guidehouse's Commercial Healthcare segment, based out of the Miami office. Erik has over 25 years of experience in healthcare leadership roles, including vendor, industry, and advisory.

He is the Director of Guidehouse's Commercial Health IT Advisory practice in North America. He was previously the healthcare cybersecurity director at Amazon and prior to that served as the Chief Information Officer at Columbia University Medical Center. His expertise is focused on healthcare technology transformation initiatives leveraging cloud, automation, artificial intelligence, and data management to support value-based care implementation and to advise on the transition to new value-based IT operating models and strategies.

Erik has worked to help clients create new IT strategy and operating models and works across healthcare startups to evaluate healthcare IT products and solutions for providers and payers. He is recognized as an industry thought leader in numerous healthcare fields, including healthcare interoperability, digital health, healthcare cloud, value-based care, health information security, and population health.

Relevant Experience

- **Value-Based Care** – Advised and led multiple implementations of value-based care models at healthcare systems in inpatient and ambulatory care settings, including strategic alignment and design. Worked with multiple children's hospitals to develop and implement IT strategy and design for health IT investments to align to value-based care objectives.
- **Healthcare technology policy and implementation** – Provided strategic guidance in defining the architecture for the Nationwide Health Information Network and was nationally recognized for contributions to ONC's associated interoperability initiatives (Direct, Connect, and the Standards & Interoperability Framework).
- **Health IT & Operating Model Implementation** – Advised and led multiple healthcare systems on operating and business model changes needed to support health IT transformation. Worked as a CIO and advisor in over 100 hospitals and health systems to optimize and enhance IT, cloud, and digital health strategies.
- **Interoperability & Population Health** – Led multiple implementations across health systems and federal health agencies to support patient-driven interoperability and led vendor assessments for providers and payers on population health platform acquisition decisions.
- **Health Analytics Assessment and Implementation** – Developed analytics strategies and operating models for healthcare payers and providers to assess and implement population health and quality reporting for value-based care model implementation.
- **Healthcare Cybersecurity** – Served as Director of Healthcare Cybersecurity for Amazon Web Services (AWS) implementing internal compliance programs and external cloud security solutions.