AFL-CIO UNION LAWYERS ALLIANCE ULA

2024 Advanced ERISA Seminar
September 26, 2024

Cybersecurity in 2024

Resources

Legal Practice

ABA Cybersecurity Legal Task Force, https://www.americanbar.org/groups/cybersecurity/

ABA Resolution 609, Aug. 2023, *Urges lawyers to keep informed about new and emerging technologies and protect digital products, systems, and data from unauthorized access, use, and modification*, available at https://www.americanbar.org/news/reporter_resources/annual-meeting-2023/house-of-delegates-resolutions/609/

ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 483 October 17, 2018, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*, available at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf

ABA Model Rules of Professional Conduct, Rule 1.6: Confidentiality, available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

New York Courts, Cybersecurity, Privacy and Data Protection CLE, effective January 1, 2023, available at https://ww2.nycourts.gov/attorneys/cle/clenews.shtml

Employee Benefits

EBSA Cybersecurity Guidance (updated 2024), Compliance Assistance Release No. 2024-01, available at https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/compliance-assistance-release-2024-01

- Cybersecurity Program Best Practices
- Tips for Hiring a Service Provider
- Online Security Tips

HHS HIPAA Guidance, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html

Combined HIPAA Regulation Text (HIPAA Administrative Simplification Regulations), available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

IFEBP Cybersecurity Toolkit, https://www.ifebp.org/resources---news/toolkits/cybersecurity

Data Breach State Laws

Perkins Coie Security Breach Notification Chart, 2023, available at https://perkinscoie.com/insights/publication/security-breach-notification-chart

Foley & Lardner State Data Breach Notification Laws, 2024, available at https://www.foley.com/insights/publications/2024/07/state-data-breach-notification-laws/

Cybersecurity Standards and Certifications

AICPA-CIMA System and Organization Controls (SOC) Examinations, available at https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

International Organization for Standardization (ISO) Series 27000 Certifications, https://www.iso.org/standard/iso-iec-27000-family

National Institute of Standards and Technology (NIST) Cybersecurity Framework, available at https://www.nist.gov/cyberframework

Other / Miscellaneous

DHS Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/

FTC Data Security Guidance, https://www.ftc.gov/business-guidance/privacy-security/data-security

Microsoft 365 for Business Security Best Practices, May 31, 2024, https://learn.microsoft.com/en-us/microsoft-365/business-premium/secure-your-business-data

Multifactor Authentication:

- SANS, What is Phishing Resistant MFA?, October 6, 2022, https://www.sans.org/blog/what-is-phishing-resistant-mfa/
- CISA, Phishing Resistant MFA is Key to Peace of Mind, April 12, 2023, https://www.cisa.gov/news-events/news/phishing-resistant-mfa-key-peace-mind
- CISA Implementing Phishing-Resistant MFA Guide, available at https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

White House National Cybersecurity Strategy Implementation Plan (updated 2024), available at https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/

Attachments / Exhibits:

Sample Breach Notification Letter (New York)

Sample Vendor Questionnaire

For Questions or comments

Andrew Lin
Mooney, Green, Saindon, Murphy and Welch, PC
(202) 783-0010
alin@mooneygreen.com

Owen Rumelt
Cary Kane PLLC
(212) 871-0539
orumelt@carykanelaw.com

Sample NYS Data Security Breach Notification Letter

(Date)

Dear (name of person):

We are writing to inform you of a recent security incident at [name of organization]. This notification is sent pursuant to the New York State Information and Security Breach and Notification Act (General Business Law Section 899-aa or State Technology Law Section 208).

[Describe what happened in general terms including the date of the security incident, specific categories of personal/private information that were involved, what you are doing in response and inform the letter's recipient as to what they can do to protect themselves as indicated below.}

To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

- Equifax (888)766-0008 or www.fraudalert.equifax.com
- Experian (888) 397-3742 or www.experian.com
- TransUnion (800) 680-7289 or www.transunion.com

New York residents can also consider placing a Security Freeze on their credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at https://dos.nysits.acsitefactory.com/consumer-protection.

When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting

www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at:www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service
P.O. Box 1025281
Atlanta, GA 30348-5283

For more information on identity theft, you can visit the following websites: New York Department of State Division of Consumer Protection:www.dos.ny.gov/consumer-protection; the Office of the NYS Attorney General at:www.ag.ny.gov; or the Federal Trade Commission at:www.ftc.gov/bcp/edu/microsites/idtheft/

If there is anything [name of your organization and website] can do to further assist you, please call [name] and [phone number].

Very truly yours,

(To be typed on Fund letterhead)

DATE

[name and address of service provider]

Dear _____;

The Employee Benefits Security Administration ("EBSA") has issued "best practices" for cybersecurity which apply to all recordkeepers and service providers that maintain personal data on ERISA fund participants and beneficiaries or have physical or functional control of ERISA plan assets. The Trustees of the NAME OF FUND, as fiduciaries, wish to ensure that your firm complies with these best practices.

Please review the attached certification, execute it, and return it to the Fund Office as soon as practicable. If you are unable to certify to any matters stated therein, please let the Trustees know.

If you have any questions, please do not hesitate to contact me.

Very truly yours,

NAME
TITLE

CERTIFICATION OF CYBERSECURITY COMPLIANCE

This certification is made by [name of service provider] ("Provider"), a provider of certain services to the NAME OF FUND (the "Fund").

In the course of providing services to the Fund, Provider may receive or have access to certain sensitive and/or confidential electronically stored or accessed information of the Fund, personally identifiable health information about Fund participants, beneficiaries and/or dependents ("Members"), or physical or functional control of plan assets of the Fund (collectively, "Protected Information"). Provider will take all commercially reasonable steps to safeguard Protected Information in its possession or control or to which it has access and will act to protect such information from unauthorized disclosure, in accordance with state and federal laws and regulations and this Certification. Such steps shall include the following:

1. Maintaining a written cybersecurity program which has been approved by and is managed by the Provider's senior leadership (the "Program"). The Program shall (1) identify and assess internal and external cybersecurity risks, (2) implement information security policies, procedures, guidelines and standards to protect the security of Provider's IT infrastructure and data and (3) document the particular framework(s) used to assess the security of Provider's systems and practices. In particular, the program shall contain policies and procedures on:

    a. Risk identification, management and protection for assets, information and systems;
    b. Detection of, response to and recovery from cybersecurity events;
    c. Disclosure of cybersecurity events as appropriate;
    d. Restoration of normal operations and services after cybersecurity events;
    e. Data governance and classification;
    f. Access to systems, including identity management procedures;
    g. Systems configuration and operation;
    h. Vulnerability and patch management;
    i. Data privacy;
    j. Data retention and disposal; and
    k. Annual cybersecurity awareness training for all personnel.

2. Designating or retaining qualified personnel, including third parties, with appropriate training, experience and certifications to undertake acts in furtherance of the Program. Provider will perform initial and periodic background checks of all such personnel.

3. Reviewing the Program annually to identify necessary updates which are then implemented in a timely manner.

4. Performing, or causing to be performed a prudent annual risk assessments of Provider's electronic systems to identify, estimate and document information system risks. Provider shall

codify the scope and methodology for each such assessment. Provider shall implement all changes necessary to mitigate or eliminate risks identified during the assessment in a timely manner.

5. Retaining an independent party to perform an annual audit of security controls. The auditor shall document its audit report and files, penetration testing reports and supporting documents, and any other analyses it performs in accordance with appropriate standards. Provider will update its processes and systems as necessary to mitigate or eliminate issues, problems or risks identified during the audit and documents such corrections and changes.

6. Initiating and maintaining systems and processes to ensure that Protected Information may only be accessed by appropriate personnel. Such processes must ensure, at a minimum, that:

    a. Access to systems and information is limited to authorized users, processes, devices, activities, and transactions;
    b. Access privileges are limited based on the roles of the individual and on a "need-to-access" basis;
    c. Access privileges are reviewed at least every three months and accounts are disabled or deleted as appropriate;
    d. Multi-factor authentication is required wherever possible;
    e. Activity by authorized users is monitored for unauthorized access, use of, or tampering with Protected Information;
    f. Protected Information about a participant, beneficiary or dependent in Provider's records matches the information that the Fund retains about that individual; and
    g. If Fund assets are to be transferred to an entity or individual, the identity of the authorized recipient of those assets is confirmed prior to transfer.

7. Performing appropriate security review and periodic assessments of third parties that manage Fund assets or data for Provider, including parties through which information is stored in the "cloud". Such third parties must have implemented appropriately documented cybersecurity and risk assessment practices which include access control policies and procedures, including multi-factor authentication and encryption. They must also agree, in writing, to notify Provider of any possible or known unauthorized access or disclosure of Protected Information.

8. Implementing security assurance programs which include annual penetration testing, regular vulnerability scans, code review and architecture analysis.

9. Written plans for business continuity, disaster recovery and incident response if a cybersecurity event occurs which:

    a. Reasonably define the internal processes for responding to a cybersecurity event or disaster;
    b. Reasonably define plan goals;

c. Define the documentation and reporting requirements for cybersecurity events and responses;
d. Clearly define and describe the roles, responsibilities and authority levels;
e. Describe internal and external communications and information sharing, including protocols to notify the Fund and affected individuals of cybersecurity incidents and events;
f. Identify remediation plans for any identified weaknesses in information systems;
g. Include after action reports on how plans will be evaluated and updated after a cybersecurity event or disaster; and
h. Are annually tested based on possible risk scenarios.

10. Encrypting sensitive data that is stored or in transit.

11. Maintaining appropriate technical controls including up to date, well maintained hardware, software, firmware, firewalls, intrusion detection programs, antivirus and antimalware programs.

12. Establishing network segregation for critical networks.

13. Routinely backing up data.

14. Maintaining and following written procedures for investigating, remediating and providing notice of a cybersecurity incident or breach.

Dated: _____, 202__

By:_____

Name:

Title: