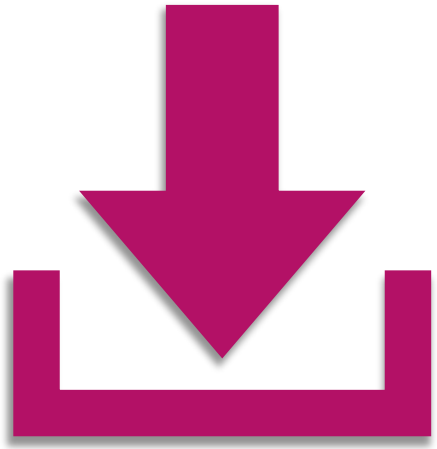
Implementing New Requirements Under Regulation S-P

INVESTMENT ADVISER REPRESENTATIVE CONTINUING EDUCATION

SPONSORED BY RIA COMPLIANCE CONSULTANTS, INC.

Download Our Slides

https://www.ria-compliance-consultants.com/Implementing-Reg-SP



Important Disclosures

Please carefully review the following disclosures and limitations of this course.

- Although the sponsor of this course, RIA Compliance Consultants, Inc. ("Sponsor"), is an affiliate of a law firm and Sponsor may have an individual on its staff that is also licensed as an attorney providing legal services in a completely separate capacity, Sponsor is **not** a law firm and does **not** provide legal services or legal advice. A consulting relationship with Sponsor does not provide the same protections as an attorney-client relationship.

- This course is offered for educational purposes only and should not be considered an engagement with Instructor or Sponsor. This presentation should not be considered a comprehensive review or analysis of the topics discussed today. These educational materials are not a substitute for consulting with an attorney or compliance consultant in a one-on-one context whereby all the facts of your situation can be considered in their entirety.



Key Point: *Taking this educational course does not create an attorney-client relationship or a compliance consulting relationship between you and your Instructor or the program Sponsor. If you have questions about your particular circumstances, we encourage you to discuss them with your compliance professional and/or your attorney.*

Please Read Our Fine Print

- Instructor and Sponsor make all reasonable efforts to ensure the educational material is current and accurate at the time of presentation. Instructor and Sponsor are not be under an obligation to advise you of any regulatory developments or subsequent changes to educational material presented in this IAR CE course.

- Information provided during this course is provided "as is" without warranty of any kind, either express or implied, including, without limitation, warranties and merchantability, fitness for a particular purpose, or non-infringement. Instructor and Sponsor assume no liability or responsibility for any errors or omissions in the content of the presentation.

- There is no guarantee or promise that concepts, opinions and/or recommendations discussed will be favorably received by any particular court, arbitration panel or securities regulator or result in a certain outcome.



Key Point: *Laws and regulations change over time, and it is impossible to predict how a court, arbitration panel, or securities regulator will act in the future. After taking this course, you should be alert for future regulatory developments.*

Keep in Mind…

- Communication with Instructor is not protected from discovery by third-parties during litigation or regulatory proceedings. Please keep questions during this course in a hypothetical form.

- Reviewing the slides and/or attending this course does not create a consulting engagement with RIA Compliance Consultants, Inc. A consulting relationship can be established only after the following two events have been completed: (1) our thorough review with you of all the relevant facts pertaining to a potential engagement; and (2) the execution of a written engagement and fee agreement and our advance receipt of any retainer required under such an agreement. The slides and/or course should not be regarded as a complete analysis of the subjects discussed. The information on these slides and in the course should not be relied upon as a substitute for one-on-one compliance advice. Often times, a party needs professional advice that applies to his or her specific situation. Your investment adviser firm should retain a compliance professional and/or attorney to provide you with specific guidance regarding your firm's situation.



Key Point: *Do not disclose confidential or proprietary information during this course. If you have questions about your particular circumstances, we encourage you to discuss them with your compliance professional and/or your attorney.*

Jurisdictions Requiring IAR CE

Already Effective As Of 1/1/24:

AR; CA; CO; DC; FL; HI; KY; MD; MI; MS; NV; ND; OK; OR; SC; TN; VT; & WI.

Effective On 1/1/25:

Minnesota; Nebraska; New Jersey; Rhode Island and U.S. Virgin Islands



Investment Adviser Rep Continuing Education

This Course Has Been Approved by NASAA For 1 Hour of IAR CE Under Ethics Category

NASAA Disclosure

NASAA does not endorse any particular provider of investment adviser representative continuing education courses. The content of this course and any views expressed are our own and do not necessarily reflect the views of NASAA or any of its member jurisdictions.



Course Requirements

- **Login** - You must be logged in during the presentation under your email address.
- **View Entire Presentation** – You are required to watch the entire presentation the course.
- **Attendance Codes** - As you watch the presentation, you will receive two attendance codes, each containing three alphanumeric characters. Save these codes. You will need to enter the full six-character attendance code prior to accessing the final quiz.
- **Login** – You will need to login into *https://www.CE4Advisers.com* and select/purchase this course.
- **IAR Acknowledgement** – Sign the IAR CE Acknowledgement & Attestation.
- **Final Quiz -** You must complete each lesson and receive a score of **70%** on the final quiz to receive IAR CE credit (assuming the course has been approved by NASAA).

Content Questions & Technical Help

If you have questions about the content of this course or need technical help, please contact us via the email address below:

ContEd@ria-compliance-consultants.com

Your Instructor



Bryan Hill, President
RIA Compliance Consultants, Inc.

Bryan has over 28 years of experience working with investment advisers, broker-dealers and investors as a compliance consultant, attorney and executive.

bhill@ria-compliance-consultants.com
877-345-4034 x 101

Jarrod James

- Senior Vice President of RIA Compliance Consultants, Inc.
- Investment Adviser Certified Compliance Professional®
- Masters of Arts in Management

jjames@ria-compliance-consultants.com

877-345-4034 x 103



Regulatory Resources

Federal Register: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Info: *https://www.federalregister.gov/documents/2024/06/03/2024-11116/regulation-s-p-privacy-of-consumer-financial- information-and-safeguarding-customer-information*

SEC Fact Sheet Final Rules: Enhancements to Regulation S-P: *https://www.sec.gov/files/34-100155-fact-sheet.pdf*

SEC Final Rule Release (Regulation S-P: Privacy of Consumer Financial Information & Safeguarding Customer): *https://www.law.cornell.edu/cfr/text/17/275.206(4)-7*

Limitations & Exclusions

- Limited to Investment Adviser Firms Registered with SEC
- Does Not Address Requirements of Broker-Dealers or Transfer Agents
- RCC Is Not a Cybersecurity Consultant

Investment Advisers Only Registered with State Securities Regulators

Regulation S-P and These Amendments Do Not Apply to Firms Which Are Only Registered with State

States May Have Similar Requirements

These Requirements Will Likely Become Best Practices/Expectations Even If Not Explicitly Listed in State Rule

Course Overview

- Incident Response Program
- Client Notification
- Service Provider
- Annual Privacy Notice Delivery
- Disposal of Customer Information
- Compliance Date

Incident Response Program

Reasonably Designed To Detect, Respond To, And Recover From Unauthorized Access To Or Use Of Customer Information

Rule Provides Flexibility in Designing IRP

Rule Amendments Require Incident Response Program To Contain Certain General Elements But Will Not Prescribe Specific Steps That Must Be Undertaken When Carrying Out Response Activities



Incident Response Program Assessment

- Procedures for Assessing Nature and Scope of Any Incident Involving Unauthorized Access or Use of **Customer Information**
- Identify Customer Information Systems & Types of Customer Information Accessed
  - *Will Help Develop A Contextual Understanding of Circumstances Surrounding Incident*
  - *Assessment Should Guide Incident Response Activities*
  - *Further Identify & Evaluate Existing Vulnerabilities for Elimination*



Incident Response Program
Contain & Control



Take Appropriate Steps To Contain And Control The Incident To Prevent Further Unauthorized Access To Or Use Of Customer Information



Objective Is To Prevent Additional Damage From Unauthorized Activity And To Reduce The Immediate Impact Of An Incident By Removing The Source Of The Unauthorized Activity



Strategies For Containing And Controlling An Incident Vary Depending Upon The Type Of Incident

Contain & Control Examples

- Isolating Compromised Systems
- Enhancing The Monitoring Of Intruder Activities
- Searching For Additional Compromised Systems
- Changing System Administrator Passwords
- Rotating Private Keys
- Changing Or Disabling Default User Accounts & Passwords

Documentation Necessary for Each Incident

- Incident Details
- Steps Taken
- Timeline Of Actions
- Personnel Involved
- Notifications (Client, Regulator, Custodian, Etc.)
- Post-incident Remediation

Customer Notification

Must Notify Each Affected Individual Whose Sensitive Customer Information Was, Or Was Reasonably Likely To Have Been, Accessed Or Used Without Authorization

Customer Notification Exception

- After Reasonable Investigation
- Determination by Investment Adviser That **Sensitive** Customer Information Has Not Been, And Is Not Reasonably Likely To Be, Used
- In A Manner That Would Result In Substantial Harm Or Inconvenience

Sensitive Customer Information

Any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information.



Examples of Sensitive Customer Information

- Social Security Number
- Driver's License Number
- Alien Registration Number
- Employer or Taxpayer Identification Number
- Biometric Record
- Unique Electronic Id Number, Address or Routing Code
- Account Number
- User Id
- Authenticating Information (E.G., Access Code, Credit Card Expiration Date, Partial SSN, Security Code, Security Q&A, DoB, Mother's Maiden Name)

Reasonable Investigation

- Depends Upon Circumstances
  - ✓ Internal Access versus External Intrusion
  - ✓ Duration of Incident
  - ✓ Accounts Accessed & At What Privilege Level
  - ✓ Whether & What Type of Customer Information Was Copied, Transferred or Retrieved
- Intentional Intrusion By Threat Actor May Require More Extensive Investigation Than Inadvertent Access By Employee
- Cannot Avoid Notification Due To Inconclusive Investigation Results



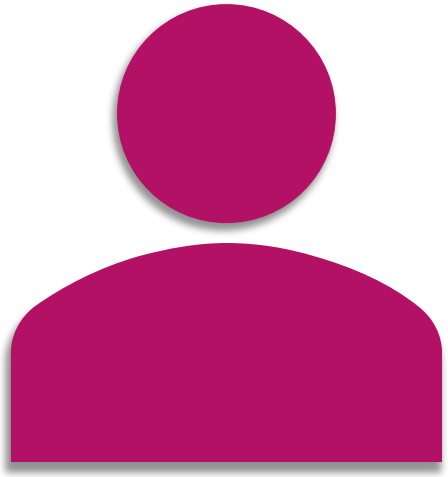
Clear & Conspicuous Notice



Must Provide **Clear & Conspicuous Notice, Or Ensure That Such Notice Is Provided**, To Each Affected Individual Whose **Sensitive Customer Information** Was, Or Is Reasonably Likely To Have Been, Accessed Or Used Without Authorization

Unable to Identify Specific Individuals

If Unable To Identify Which Specific Individuals' Sensitive Customer Information Has Been Accessed Or Used Without Authorization, Then Investment Adviser **Must Provide Notice To All Individuals Whose Sensitive Customer Information Resides** In The Customer Information System That Was, Or Was Reasonably Likely To Have Been, Accessed Or Used Without Authorization



Timing of Notification: No Later Than 30 Days

Notice Must Be Provided To Affected Individuals As Soon As Practicable, ***But Not Later Than 30 Days, After Becoming Aware*** *That Unauthorized Access To Or Use Of* ***Sensitive Customer Information*** *Has Occurred Or Is Reasonably Likely To Have Occurred*

National Security & Public Safety Exception to Customer Notification

- **Initial Notice Delay**: If the U.S. Attorney General determines that the required notice poses a substantial risk to national security or public safety, the notice may be delayed for a period specified by USAG, up to 30 days.
- **Written Notification**: The determination of risk and the decision to delay the notice must be communicated to the SEC in writing by USAG.
- **Additional Delay**: The notice may be delayed for an additional period of up to 30 days if USAG again determines that the notice continues to pose a substantial risk and provides written notification to SEC.
- **Final Delay in Extraordinary Circumstances**: In extraordinary circumstances, the required notice may be delayed beyond the initial and additional periods, as determined necessary by USAG.

Customer Notification Content

- Date & Description of Incident Including Type of Sensitive Information Accessed or Used
- Contact Information (Toll-Free Number, Email Address, Postal Address & Contact Person)
- Recommendation To Review Account Statements & Report Any Suspicious Activity
- Explanation How To Place A Fraud Alert in Credit Report
- Recommendation To Periodically Obtain Credit Report
- Information regarding FTC & Encouragement to Report Incidents to FTC
- Steps An Affected Individual Can Take To Protect Against Identity Theft

Service Provider Definition

*Any Person Or Entity (**Including An Affiliate)** That Receives, Maintains, Processes, Or Otherwise Is Permitted Access To Customer Information Through Its Provision Of Services Directly To An Investment Adviser*



Service Provider Must Protect & Notify



Service Provider Must Protect Against Unauthorized Access To Or Use Of Customer Information **And Provide Notification To The Investment Adviser As Soon As Possible, But No Later Than 72 Hours After Becoming Aware Of A Breach In Security** Has Occurred Resulting In Unauthorized Access To A Customer Information System Maintained By The Service Provider

Investment Adviser Must Ensure Appropriate Measures Taken by Service Provider

Rule Doesn't Specifically Require Contractual Agreement Between Service Provider and Investment Adviser

Rule Requires Investment Adviser's Incident Response Program's Policies and Procedures To Be ***Reasonably Designed to Ensure***

Protect Against Unauthorized Access Of Customer Information	Provide Notification Within 72 Hours Of Becoming Aware Of Breach of Customer Information System

Service Provider's Notice Triggers IA's Incident Response Program

Upon Receipt Of Service Provider's Notification Of Unauthorized Access, Investment Adviser Firm Must Initiate Its Incident Response Program

Investment Adviser Firm Needs To Ensure Affected Individuals (Subject to Unauthorized Access or Use of Sensitive Customer Information) Are Timely Notified Of Incident

IA May Enter Into Written Agreement With SP To Notify Affected Individuals

- IA Must Ensure That Affected Individuals (Subject to Unauthorized Access or Use of Sensitive Customer Information) Are Notified Of Incident (Even When Using SP to Notify)
- IA's Policies And Procedures Should Include Steps For Conducting Reasonable Due Diligence To Confirm SP Has Notified Affected Individuals
  - *Copy Of Notification & List Of Affected Clients Receiving Notification*
  - *Attestation By SP That Notification Was Sent To Affected Clients*
  - *Confirmation With A Sample of Affected Individuals That Notification Was Received*

Exception for Delivery of Annual Privacy Notice

- Only Provides Nonpublic Personal Information to Nonaffiliated Third Parties in Accordance with § 248.13 (Service Providers & Joint Marketing), § 248.14 (Processing & Servicing Transactions), or § 248.15 (Other Exceptions) **and**
- Have Not Changed Policies And Practices With Regard To Disclosing Nonpublic Personal Information From The Policies And Practices That Were Disclosed To The Customer
- To Extent Investment Adviser Changes Its P&P With Respect to Disclosing Nonpublic Personal Information, Investment Adviser With Need to Provide Customers with Privacy Notice – See Rule For Specific Details

P&P for Due Diligence of Service Providers

Investment Adviser Should Establish, Maintain And Enforce Written Policies And Procedures Reasonably Designed To Require Oversight, Including Through Due Diligence On And Monitoring, Of Service Providers, Including To Ensure That The Investment Adviser Satisfies The Customer Notification Requirements

Update Compliance Manual

Due Diligence of Service Providers

- Your Service Provider Due Diligence Section Must Include:
- Initial Due Diligence & Ongoing Due Diligence
- Contract/Written Assurance Requirements
- 72-hour Breach Notification Requirement
- Verification That Vendor Notified Affected Individuals (If Delegated)

Recommended/Required Vendor Contract or Written Assurance Terms

- Protect Against Unauthorized Access/Use
- Maintain Information Security Plan
- Notify Adviser Of Breach Within 72 Hours
- Prohibit Improper Data Use
- Secure Disposal
- No Retention Of Data After Termination
- No Ownership/Security Interest In Adviser Data
- Notify Adviser If Served With Legal Process

Example of Written Assurance for Incident Notification within 72 Hours

Microsoft: Security Incident Management Overview

https://learn.microsoft.com/en-us/compliance/assurance/assurance-incident-management

Ongoing Vendor Due Diligence

- Confirmation That Annual Assessment of Information Security Plan Was Completed and Any Issues Remediated
- Copy of Most Recent SOC 2 Report (If Applicable)
- Require Disclosure of Any Cybersecurity Incidents
- Update on Any Information Security Policies As Relates To Previous Assurances

Definition of Disposal

- Discarding Or Abandonment Of Consumer Information Or Customer Information; Or

- Sale, Donation, Or Transfer Of Any Medium, Including Computer Equipment, On Which Consumer Information Or Customer Information Is Stored

Disposal of Customer Information

Must Properly Dispose Of Customer Information By Taking Reasonable Measures To Protect Against Unauthorized Access To Or Use Of Information In Connection With Disposal

Must Adopt And Implement Written Policies And Procedures Addressing Proper Disposal Of Customer Information

Update Compliance Manual

Secure Disposal



Document how devices/media are wiped



Use industry-recognized disposal procedures



Require cloud vendors to delete data upon request/termination



Obtain certificates of destruction when possible

Refresh Information Security Plan

Recommended Topics

- Administrative, Technical, Physical Safeguards
- Access Controls & MFA
- Encryption At Rest & Transit
- Logging And Monitoring
- Device Security & Secure Disposal
- Risk Assessment Framework
- Service Provider Oversight
- Annual Review

Compliance Dates

Small Firm

Investment Adviser Registered with SEC and Less Than $1.5 Billion of Assets Under Management:

June 3, 2026

Large Firm

Investment Adviser Registered with SEC and $1.5 Billion of Assets Under Management or Greater:

December 3, 2025

Action Steps

Update Compliance Manual To Include An Incident Response Program And New Due Diligence Requirements For Service Providers With Access To Customer Information, Privacy Notice Delivery & Disposal of Customer Information – Refresh Information Security Plan

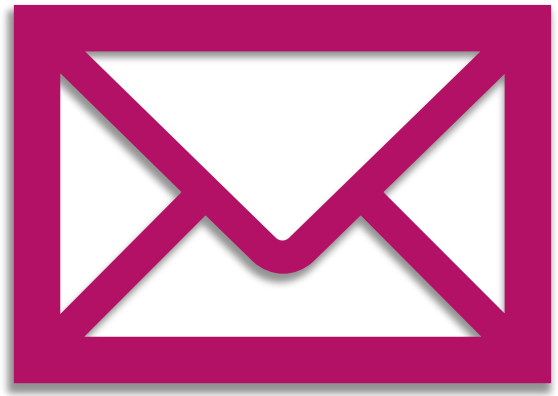
Update Agreements With Service Providers To Protect Sensitive Customer Information, Notify (Within 72 Hours) Investment Adviser Of Any Incidents And Whether And How Service Provider Will Notify (Within 30 Days) The Client Of Any Breaches

Update Initial And Ongoing Due Diligence Questionnaires Of Service Providers With Access To Sensitive Customer Information As Related To Cybersecurity And Breaches

Train Applicable Staff Members Of New Requirements

Questions

Please submit any question online or email with any questions about the content of this course.



ContEd@ria-compliance-consultants.com

Thank You

