RadarFirst

CYBERSECURITY NOTIFICATION OBLIGATIONS

Financial Services | U.S. Federal

Disclaimer

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this presentation are for general informational purposes only. Information in this presentation may not constitute the most up-to-date legal or other information. This presentation contains links to third-party websites. Such links are only for the convenience of the reader; RadarFirst does not recommend or endorse the contents of the third-party sites.

INTRODUCTION

When cyber incidents occur, organizations have a responsibility to report them to various agencies, partners, and stakeholders.

In a recent report, the Department of Homeland Security found that there are **52 cyber incident reporting requirements, either in effect or proposed, across the Federal Government and 22 agencies**.

Current requirements are derived from a patchwork of regulations and authorities, many with unique and sometimes overlapping information requirements, timelines, and submission methods.

To simplify U.S. Federal reporting for Financial Services organizations, RadarFirst has collected the following 21 effective and proposed reporting requirements for cybersecurity notification obligations, their timelines, triggers, and reporting thresholds.

RadarFirst

REGULATIONS

CFTC
- 17 C.F.R. part 37, subpart O*
- 17 C.F.R. part 38, subpart U*
- 17 C.F.R. part 39, subpart B*
- 17 C.F.R. § 49.24*

FDIC
- 12 C.F.R. part 304, subpart C**
- 12 C.F.R. part 364, app. B**

FRB
- 12 C.F.R. §§ 225.300-225.303**
- 12 C.F.R. part 208, app. D-2, 12 C.F.R part 225, app. F**

FinCEN (DoT)
- 31 C.F.R. chapter X*

FHFA
- Advisory Bulletins (Abs): AB 2020-05, Enterprise Cybersecurity Incident Reporting; AB 2017-02, Information Security Risk Management 12 C.F.R. part 1214**

FTC
- Standards for Safeguarding Customer Information**

NCUA
- 12 C.F.R. part 748, apps. A, B****

OCC
- 12 C.F.R. part 53**
- 12 C.F.R. part 30, app. B***

SEC
- 17 C.F.R. §§ 242.1002, 242.1003**
- Regulation S-P: Privacy of Consumer Financial Information (“Reg. S-P”)
- Regulation S-ID: Identity Theft Red Flags (Reg. S-ID
- Amendments Regarding the Definition of “Exchange” and Alternative Trading Systems (“ATSs”) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities (*Proposed*)**
- Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (*Proposed*)**
- Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*
- Cybersecurity Risk Management Rule (*Proposed*)***

* ***Obligation includes urgent notification, i.e. “promptly” or “as soon as possible.”***

* ***Obligations includes time-based notification.***

** / **/ ** ***Regulation includes multiple obligations unique timelines and/or unique recipients.***

RadarFirst

Commodity and Futures Trading Commission (CFTC)

Requirement

CFTC (17 C.F.R. part 37, subpart O)

Entities Subject to Reporting Requirements → Timeline and Triggers

Swap Exchange Facilities

→ Must notify the CFTC **"promptly"** as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Reportable Cyber Incidents / Threshold

Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality, or integrity of data.

A swap execution facility shall notify Commission staff promptly of all:

(1) Electronic trading halts and material system malfunctions;

(2) Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and

(3) Activations of the swap execution facility's business continuity-disaster recovery plan.

RadarFirst

Commodity and Futures Trading Commission (CFTC)

Requirement

CFTC (17 C.F.R. part 38, subpart U)

Entities Subject to Reporting Requirements → Timeline and Triggers

Designated Contract Markets

→ Must notify the CFTC **"promptly"** as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Reportable Cyber Incidents / Threshold

Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

A designated contract market must notify Commission staff promptly ***(in hours not days)*** of all:

- Electronic trading halts and significant systems malfunctions;
- Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and
- Activation of the designated contract market's business continuity-disaster recovery plan.

A designated contract market must give Commission staff timely advance notice of all material:

- Planned changes to automated systems that may impact the reliability, security, or adequate scalable capacity of such systems; and
- Planned changes to the designated contract market's program of risk analysis and oversight.

RadarFirst

Commodity and Futures Trading Commission (CFTC)

Requirement

CFTC (17 C.F.R. part 39, subpart B)

Entities Subject to Reporting Requirements → Timeline and Triggers

Derivatives Clearing Organizations

→ Must notify the CFTC **"promptly"** as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Reportable Cyber Incidents / Threshold

Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

Notice of exceptional events. A derivatives clearing organization shall notify staff of the Division of Clearing and Risk, or any successor division, promptly of:

- Any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity; or
- Any activation of the derivatives clearing organization's business continuity and disaster recovery plan.

Notice of planned changes. A derivatives clearing organization shall provide staff of the Division of Clearing and Risk, or any successor division, timely advance notice of all material:

- Planned changes to the derivatives clearing organization's automated systems that may impact the reliability, security, or capacity of such systems; and
- Planned changes to the derivatives clearing organization's program of risk analysis and oversight.

RadarFirst

Commodity and Futures Trading Commission (CFTC)

Requirement

CFTC (17 C.F.R. § 49.24)

Entities Subject to Reporting Requirements → Timeline and Triggers

Swap Data Repositories

→ Must notify the CFTC **"promptly"** as important information becomes available, and to provide a full report once the entity's investigation is complete. There is a credentialed portal provided to registrants.

Reportable Cyber Incidents / Threshold

Cybersecurity incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity, or the availability, confidentiality or integrity of data.

A swap data repository shall notify Commission staff promptly of all:

- Systems malfunctions;
- Cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security, or capacity; and
- Any activation of the swap data repository's business continuity-disaster recovery plan.

Appendix A provides guidance on the development and implementation of member information security programs including the **creation of response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies**.

RadarFirst

Department of the Treasury (DoT)

Requirement

FinCEN (31 C.F.R. chapter X)

Entities Subject to Reporting Requirements → Timeline and Triggers

Financial Institutions

→ Must notify the DoT **no later than 30 calendar days after the activity is detected with a maximum extension of 30 additional days**.

Reportable Cyber Incidents / Threshold

Suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets.

RadarFirst

Federal Deposit Insurance Corporation (FDIC)

Requirement

FDIC (12 C.F.R. part 304, subpart C)

Entities Subject to Reporting Requirements → Timeline and Triggers

Entities subject to direct supervision by the FDIC. Also includes "Bank service providers," which are required to provide notice of certain "computer-security incidents" to their customers that are banking organizations.

→ Must notify the FDIC **as soon as possible, and no later than 36 hours after the banking organization determines that a notification incident has occurred**.

→ Must provide notice to each affected customer that is a banking organization **as soon as possible when it determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.**

Reportable Cyber Incidents / Threshold

Computer-security incident: an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

Notification Incident: a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's -

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

RadarFirst

Federal Deposit Insurance Corporation (FDIC)

Requirement

FDIC (12 C.F.R. part 364, app. B)

Entities Subject to Reporting Requirements → Timeline and Triggers

All insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

→ Must notify primary federal regulator **as soon as possible** when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.

→ Must notify customers **as soon as possible** when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.

Reportable Cyber Incidents / Threshold

An incident involving unauthorized access to or use of sensitive customer information, as defined below.

Sensitive customer information: a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account.

Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number.

RadarFirst

Federal Reserve Board (FRB)

Requirement

FRB (12 C.F.R. §§ 225.300-225.303)

Entities Subject to Reporting Requirements → Timeline and Triggers

"Banking organizations" must notify the Board of "notification incidents". Banking organizations for the Board include U.S. bank holding companies; U.S. savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and Edge or agreement corporations; provided, however, that no designated financial market utility shall be considered a banking organization. "Bank service providers" are required to provide notice of certain "computer-security incidents" to their affected banking organization customers. The rule carves out designated financial market utilities, those entities are subject to separate requirements promulgated by the Federal Reserve Board.

→ Must notify the Board **as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.**

→ Must notify each affected banking organization customer **as soon as possible** when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

→ Must notify each affected banking organization customer **as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours**.

Reportable Cyber Incidents / Threshold

Computer-security incident: an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

Notification Incident: a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's -

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

RadarFirst

Federal Reserve Board (FRB)

Requirement

FRB (12 C.F.R. part 208, app. D-2, 12 C.F.R part 225, app. F)

Entities Subject to Reporting Requirements → Timeline and Triggers

State member banks and their nonbank subsidiaries (except for brokers, dealers, persons providing insurance, investment companies, and investment advisors); Edge and agreement corporations, and uninsured state-licensed branches or agencies of a foreign bank; and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Board has supervisory authority.

→ Must notify primary Federal regulator **as soon as possible** when the institution becomes aware of an incident involving unauthorized access to or use sensitive customer information.

→ Must notify customers when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, **the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible**.

Reportable Cyber Incidents / Threshold

Sensitive customer information: a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account.

Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number.

RadarFirst

Federal Housing Finance Agency (FHFA)

Requirement

FHFA (Advisory Bulletins): AB 2020-05, Enterprise Cybersecurity Incident Reporting;

AB 2017-02, Information Security Risk Management 12 C.F.R. part 1214)

Entities Subject to Reporting Requirements → Timeline and Triggers

No regulatory requirement. This guidance is applicable to Freddie Mac and Fannie Mae (Enterprises); Federal Home Loan Banks; Office of Finance

→ Must identify triggers and establish timing for incident notifications. For the Enterprises, FHFA expects **immediate notification after incident detection for major incidents and 24-hour notification for significant incidents**.

Guidance directs regulated entities to maintain communication protocols; Enterprises should update reports periodically and include a description of the incident

Reportable Cyber Incidents / Threshold

An occurrence that:

- Occurs at an Enterprise or at a third party that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Enterprise system or Enterprise information the system processes, stores, or transmits; or
- Constitutes a violation or imminent threat of violation of the Enterprise's security policies, security procedures, or acceptable use policies.

RadarFirst

Federal Trade Commission (FTC)

Requirement

Standards for Safeguarding Customer Information

Entities Subject to Reporting Requirements → Timeline and Triggers

"Financial institutions" under the Rule, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that aren't required to register with the SEC.

→ Must notify the FTC **as soon as possible, and no later than 30 days** after discovery, of a security breach involving the information of at least 500 consumers if unencrypted customer information has been acquired without the authorization of the individual to which the information pertains. The notice to the FTC must include certain information about the event, such as the number of consumers affected or potentially affected.

→ Must notify the Board of Directors or governing body. Your Qualified Individual must **report in writing regularly – and at least annually**. If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program. What should the report address? First, it must include an overall assessment of your company's compliance with its information security program. It must also cover specific topics related to the program – e.g., risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded, and recommendations for changes in the information security program.

Reportable Cyber Incidents / Threshold

Notification event: when there is "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains."

Customer information: means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Nonpublic personal information means:

- Personally identifiable financial information; and
- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

Security event: an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

Service provider: any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

RadarFirst

National Credit Union Administration (NCUA)

Requirement

NCUA (12 C.F.R. part 748, apps. A, B)

Entities Subject to Reporting Requirements → Timeline and Triggers

Federally insured credit unions…. advises that at minimum, a credit union's response program should contain procedures for notifying the appropriate NCUA regional director

→ Must notify NCUA regional director **as soon as possible** when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information.

→ Must notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention.

→ Must notify NCUA **as soon as possible**.

→ Must notify member **as soon as possible**. If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible.

Reportable Cyber Incidents / Threshold

12 C.F.R 748, Appendix A provides guidance on the development and implementation of member information security programs including the creation of response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.

RadarFirst

Office of the Comptroller of the Currency (OCC)

Requirement

Computer-Security Incident Notification Rule (In Effect) 12 C.F.R Part 53

Entities Subject to Reporting Requirements → Timeline and Triggers

National banks; Federal savings associations; and Federal branches and Federal agencies of foreign banks
→ Must notify **as soon as possible and no later than 36 hours** after the banking organization determines that a notification incident has occurred.

"Bank Service Providers"
→ Must notify each affected customer that is a banking organization **as soon as possible** when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

Designated financial market utilities
→ Are **subject to separate requirements** promulgated by the Federal Reserve Board.

Reportable Cyber Incidents / Threshold

Computer-security incident: an occurrence that **results in actual harm to the confidentiality, integrity, or availability** of an information system or the information that the system processes, stores, or transmits.

Notification incident: a computer-security incident that has **materially disrupted or degraded, or is reasonably likely** to materially disrupt or degrade, a banking organization's:

1. Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;
2. Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or
3. Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

RadarFirst

Office of the Comptroller of the Currency (OCC)

Requirement

OCC (12 C.F.R. part 30, app. B)

Entities Subject to Reporting Requirements → Timeline and Triggers

National banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers); Entities subject to direct supervision by the FDIC. Also includes "Bank service providers."

→ Must notify Primary Federal regulator notification **as soon as possible** "when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information."

→ Must notify customers that are banking organizations **as soon as possible** of "computer-security incidents."

→ Must notify customers **as soon as possible**, after **conducting a reasonable investigation to determine the likelihood that the information has been or will be misused** and the investigation determines that misuse of its information about a customer has occurred or is reasonably possible.

Reportable Cyber Incidents / Threshold

"An incident involving unauthorized access to or use of sensitive customer information…" (12 C.F.R Part 30, App. B, Supp. A, section II.A.1.b.) and **"Notifying customers when warranted"** (12 C.F.R Part 30, App. B., Supp. A, section II.A.1.e.).

Sensitive customer information: a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account.

Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number." (Section III.A, Supplement A to Appendix B, 12 C.F.R Part 30.)

RadarFirst

Securities Exchange Commission (SEC)

Requirement

SEC (17 C.F.R. §§ 242.1002, 242.1003)

Entities Subject to Reporting Requirements → Timeline and Triggers

Designated “SCI entities” that directly support any one of six key securities market functions: trading, clearance and settlement, order routing, market data, market regulation, and market surveillance, including registered security-based swap data repositories; all clearing agencies that are exempt from registration; and certain large broker-dealers.

→ Must notify SEC **immediately** upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. (with delayed reporting permitted for SCI events with de minimis impact).

→ Must file a written notification with the SEC **within 24 hours following initial notification**.

→ Additional updates are required **until such time as the SCI event is resolved and the SCI entity’s investigation of the SCI event is closed.** (Frequency of ongoing updates are situation dependent as determined by a representative of the SEC.)

→ A final written notification is required **within five business days** after the resolution of an SCI event and closure, including details of the investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the SEC.

→ Other related reporting requirements include the requirement for SCI entities to file a **quarterly report** of systems disruptions and systems intrusions with no or a de minimis impact.

Reportable Cyber Incidents / Threshold

SCI entities are required to notify the Commission of "SCI events", defined as:

- **Systems disruptions**: an event in an SCI entity’s SCI systems that disrupts or significantly degrades, the normal operation of an SCI system;
- **Systems intrusions**: any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; and
- **Systems compliance issues**: an event at an SCI entity that has caused any SCI system to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity’s rules or governing documents

Note: "SCI Systems" are defined as all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Note: On March 15, 2023, the SEC proposed amendments to Reg. SCI that would expand the definition of systems intrusion to include a broader range of cyber incidents experienced by an SCI entity, and require additional policies and procedures to help an SCI entity ensure that relevant systems are robust, resilient, and secure.

RadarFirst

Securities Exchange Commission (SEC)

Requirement

SEC Regulation S-P: Privacy of Consumer Financial Information ("Reg. S-P") (In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Broker-dealers, investment companies and investment advisers registered with the Commission

→ Must notify affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization

Reportable Cyber Incidents / Threshold

Current Reg. S-P does not set forth any obligations to report incidents to the Commission. It does, however, set forth certain obligations regarding the provision of privacy notices to customers.

Note: On March 15, 2023, the SEC proposed amendments that would broaden Reg. S-P to require broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions") to notify affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. In addition, the proposed amendments would extend the application of the safeguards provisions in Regulation S-P to transfer agents.

RadarFirst

Securities Exchange Commission (SEC)

Requirement

SEC Regulation S-ID: Identity Theft Red Flags (Reg. S-ID) (In Effect)

Entities Subject to Reporting Requirements → Timeline and Triggers

Broker-dealers, investment companies and investment advisers that are registered with the Commission.

→ Must notify customers about its privacy policies and practice.

Reportable Cyber Incidents / Threshold

Reg. S-ID does not set forth any obligations to report incidents to the Commission. It does, however, require covered financial institutions to **provide notice to customers about its privacy policies and practice.**

RadarFirst

Securities Exchange Commission (SEC)

Requirement

Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems ("ATSs") That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities (Proposed)

Entities Subject to Reporting Requirements → Timeline and Triggers

ATSs that meet certain volume thresholds.

→ Must notify SEC **immediately** upon any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. (with delayed reporting permitted for SCI events with de minimis impact).

→ Must file a written notification with the SEC **within 24 hours following initial notification**.

→ Additional updates are required **until such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed.** (Frequency of ongoing updates are situation dependent as determined by a representative of the SEC.)

→ A final written notification is required **within five business days** after the resolution of an SCI event and closure, including details of the investigation regarding such SCI event, submit a final written notification pertaining to such SCI event to the SEC.

→ Other related reporting requirements include the requirement for SCI entities to file a **quarterly report** of systems disruptions and systems intrusions with no or a de minimis impact.

Reportable Cyber Incidents / Threshold

Same as under Reg: SCI. SCI entities are required to notify the Commission of "SCI events", defined as:

- **Systems disruptions**: an event in an SCI entity's SCI systems that disrupts or significantly degrades, the normal operation of an SCI system;
- **Systems intrusions**: any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; and
- **Systems compliance issues**: an event at an SCI entity that has caused any SCI system to operate in a manner that does not comply with the Act and the rules and regulations thereunder or the entity's rules or governing documents

Note: "SCI Systems" are defined as all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance.

Note: On March 15, 2023, the SEC proposed amendments to Reg. SCI that would expand the definition of systems intrusion to include a broader range of cyber incidents experienced by an SCI entity, and require additional policies and procedures to help an SCI entity ensure that relevant systems are robust, resilient, and secure.

RadarFirst

Securities Exchange Commission (SEC)

Requirement

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Proposed)

Entities Subject to Reporting Requirements → Timeline and Triggers

Investment advisers registered or required to be registered with the Commission, and registered investment companies and business development companies ("funds").

→ Must notify regulators **promptly, but in no event more than 48 hours**, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring.

→ Advisers must amend any previously filed Form ADV-C **promptly, but in no event more than 48 hours**, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident.

Reportable Cyber Incidents / Threshold

Cybersecurity incident: an unauthorized occurrence on or conducted through [an adviser's or a fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an adviser's or a fund's] information systems or any [adviser or fund] information residing therein.

RadarFirst

Securities Exchange Commission (SEC)

Requirement

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (In Effect on September 5, 2023)

Entities Subject to Reporting Requirements → Timeline and Triggers

Public companies subject to the reporting requirements of the Securities Exchange Act of 1934

→ Must notify regulators **within four business days** of company's determination that a cybersecurity incident is ***material***.

Reportable Cyber Incidents / Threshold

Cybersecurity incident: an unauthorized occurrence, or a series of related unauthorized occurrences, on, or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

RadarFirst

Securities Exchange Commission (SEC)

Requirement

Cybersecurity Risk Management Rule (Proposed)

Entities Subject to Reporting Requirements → Timeline and Triggers

Broker-dealers, clearing agencies, major security- based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents ("Market Entities")

→ Must notify regulators **immediate written electronic notice** of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident had occurred or is occurring.

→ Must report to the SEC **promptly (but no later than 48 hours),** following immediate electronic notice, information about the significant cybersecurity incident by filing Part I of proposed Form SCIR.

→ Must file an updated Part I of Form SCIR when information on the previously filed report materially changes or the incident is resolved or an internal investigation of the incident is concluded.

Reportable Cyber Incidents / Threshold

Significant cybersecurity incidents, defined as a cybersecurity incident, or a group of related cybersecurity incidents, that:

- Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or
- Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in:
  - Substantial harm to the market entity; or
  - Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.

RadarFirst

Enterprise Value is at Risk

Existing tools and manual processes cannot scale with today's complexity.

Challenges

- Increased incident volumes
- Changing laws and regulations
- Assessment / decision consistency
- Short notification timelines
- Stretched resource capacity

Impact

- Missed notification deadlines
- Regulatory audits and fines
- Customer loss
- Significant external legal costs
- Staff retention / attrition

Outcomes

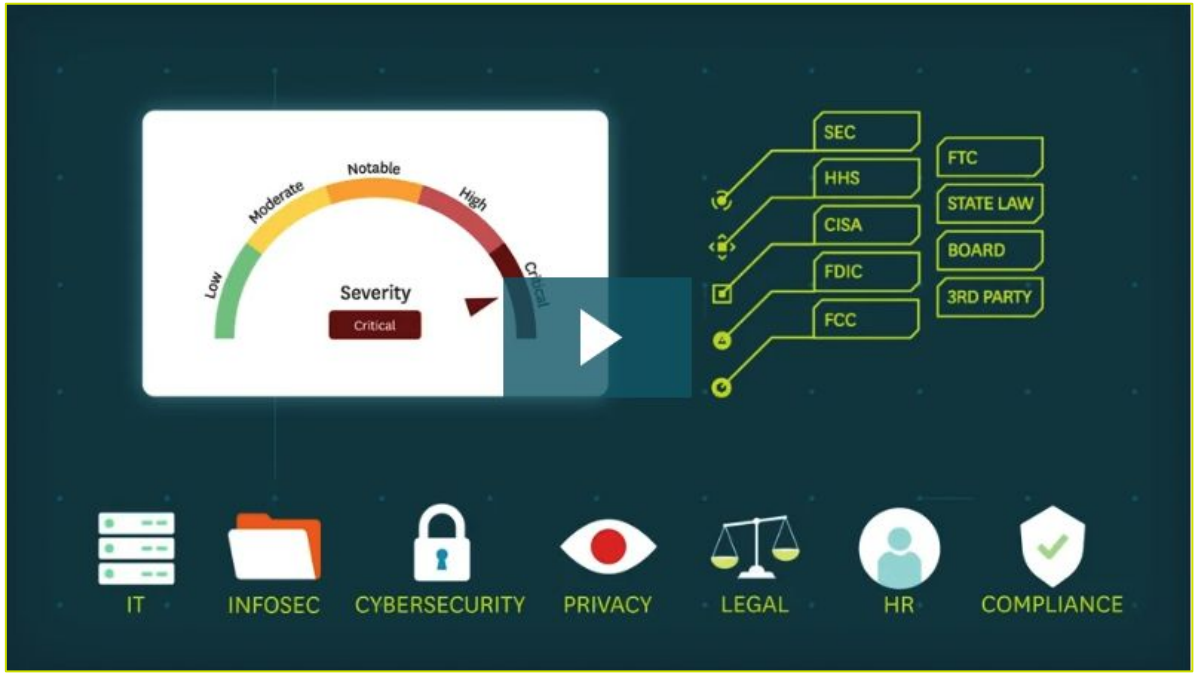
- Decreased enterprise value
- Brand / reputational damage
- Lost customer / partner loyalty
- Inability to scale
- High departmental overhead

Operationalize Notification Obligations with Radar® Compliance

Radar® Compliance is a rules and assessment engine that can be configured to satisfy internal and external compliance notification requirements and obligations, such as:

- Cybersecurity events
- Third-party contractual mgmt
- Auditable reporting
- And more

Talk to a RadarFirst specialist to learn how you can define your own notification triggers and obligations with **Radar® Compliance**.



Capital One · VOYA FINANCIAL · BNY MELLON · CNO FINANCIAL GROUP · Texas Capital Bank · RAYMOND JAMES · Hyundai Capital

Thank You!

Reduce risk and simplify obligation decisioning at radarfirst.com.

RadarFirst

Join the conversation!

@radarfirst

linkedin.com/company/radarfirst