SECURITY BASECAMP

Cybersecurity Incident Mgmt.

BEST PRACTICE GUIDANCE FOR SEC/FINRA-REGULATED FIRMS

OVERVIEW OF REGULATION S-P AMENDMENTS

Key requirements to address before the compliance date

- **Adopt and implement** an Incident Response Program.
- **Detect, respond, and recover** from unauthorized access or use of client information and prevent usage.
- **Assess, respond and contain** the incident, and prevent future unauthorized access / use.
- **Oversee and monitor** service providers.
- **Adopt and implement** a Vendor Management Program.
- **Meet customer notification requirements** in the event of a breach.
- **Notice required within 30 days** of becoming aware of unauthorized access to sensitive customer information, unless an exception is met.
- **Comply with enhanced safeguards** and disposal requirements.
- **Maintain books and records** to evidence compliance.

DETECT, TRIAGE, & CONTAIN

- Quickly **scope what's affected** (systems, data, customers), **declare severity, and isolate compromised accounts/systems while preserving evidence.** [1]
- **Activate the BCP for material service disruption** (e.g., DOS affecting operations). [1]

NOTIFY, DISCLOSE, & REPORT

- **Customer notification (Reg S-P):** Have and follow a written incident-response program. If "sensitive customer information" was (or likely was) accessed/used without authorization, **notify affected individuals as soon as practicable and no later than 30 days** after becoming aware, with prescribed content.[2]
- **Public company disclosure (if applicable):** If your firm (or parent) is a registrant,
  - **File Form 8-K Item 1.05 within four business days after determining materiality,** describing the incident's nature, scope, timing, and impact.[2]
- **FINRA reporting:** Cyber events can implicate multiple rules; where your firm concludes (or reasonably should conclude) there's a rule violation
  - **Promptly report under FINRA Rule 4530(b).**
  - **Coordinate with supervision/controls** (3110/3120), books-and-records (SEA 17a-3/4), BCP (4370)
  - **Identity-theft obligations** (Reg S-ID).[1]
- **Law enforcement and sector reporting:**
  - **Consider FBI IC3/field office, USSS, and CISA** voluntary reporting to boost asset recovery and obtain threat intel
  - **File FinCEN SARs** when activity meets Bank Security Act (BSA) thresholds.
  - Many firms also must follow **state breach-notification** laws.
  - **Build** these routes **into your IRP.**[1]

ERADICATE & RECOVER

- **Remove** footholds
- **Reset** credentials/keys
- **Rebuild** clean images
- **Validate** with monitoring
- **Watch for reinfection.** Document every step and keep a time-stamped log of decisions and artifacts. [1]

COMMUNICATE CLEARLY

- **Centralize internal/external comms** (exec sponsor + counsel + IR lead).
- Use out-of-band channels if email/chat are suspect.
- Keep messages factual, consistent, and regulator-ready.[1]

LEARN & IMPROVE

- **Practice post-incidence hardening**
- Run a **formal lessons-learned, update playbooks/policies**
- **Fix control gaps** (e.g., MFA/conditional access, vendor oversight, monitoring),
- **Retrain staff & Re-test.**[1]

SECURITY BASECAMP

Cybersecurity Incident Mgmt.

OPERATIONAL CHECKLIST

ACTIVATE IRP
- Name an incident lead
- Open case
- Start a time-stamped evidence log.[1]

NOTIFY
(Matrix below)
- Customers
- Regulators
- Public
- Federal / State / local law enforcement

MONITOR
for re-attack.

DEBRIEF & FIX
Update policies, controls, training, and vendor requirements. [1]

CONTAIN
- Isolate accounts/systems
- Preserve evidence
- Stabilize business operations/Business Continuity Plan. [1]

COMMUNICATE
- Internal: IR Lead + Exec Sponsor + Counsel. Out-of-band if core systems suspect.
- External: All customer, regulator, and vendor notices reviewed/approved by counsel.
- Consistency: Use factual, regulator-ready messaging. No speculation.

ASSESS & ESCALATE
- Impact Analysis: Determine scope (systems, data, customers, vendors).
- Severity Rating: Classify as low, medium, high, critical based on client data exposure and business impact.
- Counsel Engagement: Engage legal early to preserve privilege.

ERADICATE & RECOVER
- Remove malicious code, reset credentials/keys, rebuild clean images.
- Validate integrity and monitor for recurrence.

NOTIFCATION MATRIX

OBLIGATION	TRIGGER	DEADLINE
Reg S-P (customer notice)	Unauthorized access/use of sensitive customer info	Reg S-P (customer notice)
SEC Form 8-K (public cos.)	Incident deemed material	4 business days after materiality determination
FINRA Rule 4530(b)	Actual/possible rule violation (e.g., supervisory, BCP, safeguarding)	Promptly
Reg S-ID	Identity theft red flags detected	Immediate escalation; follow firm's written program
State Breach Law(s)	Personal info of residents compromised	Varies (often 30–45 days) – counsel to coordinate
Law Enforcement / Sector	Financial loss, fraud, ransomware, systemic threat	FBI IC3 / USSS / CISA within 72 hours recommended
FinCEN SAR	Cybercrime tied to suspicious transactions (e.g., ransomware)	Within 30 days of initial detection

Source: (1) FINRA, (2) SEC

NOTE: This Quick Guide has been created using source materials from FINRA and other regulatory bodies for information only. It is not legal or compliance advise. Firms may find this helpful as they develop new, or modifying existing, policies and procedures that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model. Some items may not be relevant due to certain firms' business models, sizes, or practices. The citation or listing of any organization should not be interpreted as endorsements of the organizations. Firms designing and implementing Incident Management policies and practices should consult their own legal and compliance professionals and/or seek outside review.