



CYBER CLAIM REPORTING & INCIDENT RESPONSE GUIDE

For VSBIT member school districts | October 2026

SUSPECTED OR CONFIRMED CYBER INCIDENT? START HERE

Immediately begin BOTH actions below, at the same time. Do not wait for one to finish before starting the other.

ACTION A | CALL THE 24/7 BREACH HOTLINE

844-885-1574

Mullen Coughlin is the breach counsel available through VSBIT's cyber insurance program.

When calling, provide:

- Your school district's name
- That you are a VSBIT member
- Chubb policy no. G75506089 001

ACTION B | REPORT THE INCIDENT TO VSBIT

Report a Claim - VSBIT (click here)

vsbit.org/vsbit-multi-line-report-a-claim/

Use the reporting page to submit the incident. VSBIT will notify Chubb on the district's behalf.

Use the appropriate reporting option for your district's login access.

Typically, after 24 hours Chubb will have assigned an adjuster and schedule a call to review the incident and coverage information.

IMPORTANT: Calling the hotline does not report the claim under the policy. Complete Action B as well.

NEXT | BREACH COUNSEL COORDINATES THE RESPONSE

Mullen Coughlin will help coordinate the next steps, including any needed forensic investigation. Arete is one of the forensic response providers available through the program.

Do not contact or hire a forensic firm or other outside response vendor without first coordinating with breach counsel, VSBIT, and Chubb.

THROUGHOUT THE RESPONSE | PRESERVE EVIDENCE & COORDINATE

- Activate your incident response team and follow the district's plan.
- Preserve logs, emails, system images, ransom notes, and other evidence.
- Do not delete, reimage, or materially alter affected systems unless directed by breach counsel or forensics.
- Coordinate external messages, notifications, law enforcement contacts, and payment decisions through breach counsel.
- Document the timeline, affected systems, actions taken, and known or suspected data impacts.

WHEN TO REPORT | WHEN IN DOUBT, REPORT

The policy requires prompt written notice of incidents or claims. Report to VSBIT as soon as possible after becoming aware of a claim or a situation that might lead to one.

If outside help is needed, report the incident and coordinate approval before hiring vendors. Reporting minor incidents does not typically affect cyber insurance renewal terms.

CYBER INSURANCE AT A GLANCE | REFERENCE INFORMATION

- Primary Chubb policy: G75506089 001 (07/01/26–07/01/27).
- Coverage may include first-party losses, third-party claims, incident response, public relations, and ransomware.
- Each district has at least \$1 million in limits; some have higher limits or ransomware restrictions.
- Each district has a \$25,000 retention (deductible) per claim.

USE FOR: ransomware, unauthorized access, compromised email, exposed personal information, system outages, fraudulent fund transfers, and alleged privacy or network security failures.

GALLAGHER CLAIMS ADVOCACY Gallagher can help with claim reporting, carrier coordination, and claims advocacy. Contact the VSBIT Team for more details.

This quick-reference guide does not amend, expand, or replace the insurance policy. Coverage is subject to all policy terms, conditions, exclusions, limits, retentions, and applicable member certificates. This is not legal advice.



CYBER INCIDENT CHEAT SHEET

Quick actions and what to know by incident type | Side 2

For claim reporting, the breach hotline, and coverage information, use Side 1: Cyber Claim Reporting & Incident Response Guide.

RANSOMWARE / EXTORTION	COMPROMISED ACCOUNT / EMAIL
• Preserve the ransom note, screenshots, attacker messages, wallet address, and threat actor/group name. • Do not negotiate or pay independently. • Preserve evidence while containing affected systems and beginning recovery. • Recovery first. Ransom payment should be a last resort when critical operations cannot reasonably be restored another way. • Payment does not undo the breach or guarantee that stolen data will be deleted or kept private.	• Disable or secure the account and reset credentials. • Revoke active sessions/tokens and review MFA methods for anything unfamiliar. • Review forwarding rules, mailbox rules, delegated access, and recent sign-ins. • Preserve logs, suspicious messages, and other evidence. • Determine whether sensitive information or other accounts/systems may have been accessed.
FRAUDULENT FUND TRANSFER / BEC	SUSPECTED DATA BREACH / UNAUTHORIZED ACCESS
• Contact the bank immediately and request a hold, freeze, or recall of the transfer. • Report the fraud to IC3.gov immediately. • Contact FBI: Leah Bogdanowicz lbogdanowicz@fbi.gov. • Preserve transfer instructions, account details, emails, invoices, and timestamps. • Speed matters. Early bank and law-enforcement involvement can improve the chance of stopping or recovering funds.	• Preserve logs and evidence and determine what information may have been accessed or acquired. • Do not independently send breach notifications or make regulatory filings before coordinating with breach counsel. • Breach counsel should determine whether Vermont reporting or individual notification requirements are triggered. • Not every cyber incident is automatically a legally reportable data breach.

LAW ENFORCEMENT - WHAT TO PROVIDE / WHAT THEY MAY HELP WITH

CONTACTS

- Vermont Intelligence Center (VIC): 802-872-6110 | dps.vic@list.vermont.gov
- FBI: Leah Bogdanowicz | lbogdanowicz@fbi.gov
- Internet Crime Complaint Center: IC3.gov (especially for fraudulent transfers/BEC)

PROVIDE WHEN AVAILABLE

- Ransom note, threat actor/group, wallet address, attacker communications, malicious IPs/domains, timestamps, and financial transfer details.

LAW ENFORCEMENT MAY BE ABLE TO HELP WITH

- Threat-actor or cryptocurrency-wallet intelligence.
- Known decryptors or information from related investigations.
- Coordination with other law-enforcement partners.
- Fraudulent fund freeze/recovery efforts.
- Evidence preservation or investigative guidance.

VERMONT BREACH REPORTING

- Breach counsel should determine whether Vermont Security Breach Notice Act requirements are triggered.
- When applicable, preliminary notice to the Vermont Attorney General is generally due within 14 business days of discovery or before consumer notice, whichever is sooner.
- Consumer notice is generally required without unreasonable delay and no later than 45 days after discovery, subject to applicable exceptions and law-enforcement needs.
- Do not wait until the end of the investigation to raise reporting questions. Timing can begin at discovery.

WHAT TO EXPECT FROM BREACH COUNSEL / FORENSICS

- Breach counsel should explain what is happening, why it matters, and what decisions the school needs to make.
- Counsel should explain Vermont reporting/notification requirements and coordinate legal and law-enforcement issues.
- Forensics should explain what they are trying to determine, what they need from the school, and how the investigation affects recovery.
- Recovery and investigation should proceed in parallel where appropriate.
- Ask questions. Members should understand the process, available resources, and next steps throughout the incident.

This cheat sheet is a quick reference and does not replace the district incident response plan, applicable insurance policy, or legal advice. Vermont reporting summary: 9 V.S.A. § 2435.