Vantalect



AWS INCIDENT RESPONSE RETAINER · SAMPLE DELIVERABLE

Activation Call Sheet

DISTRIBUTION: OPERATIONAL

Week 1 of the Retainer: Call sheet · prepared for Wrenfield Bancorp, Inc.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

August 14, 2026 · AWS Incident Response Retainer (one year)

SAMPLE DELIVERABLE

This is a sample deliverable. Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

Call in this order

At 1 AM on a holiday: page Vantalect early, counsel signs the activation, and one person runs one command. Call sheet 1.0, Friday, August 14, 2026. This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis. It decides nothing about notice, privilege, or regulators; counsel and the bank do. The August 12 drill took 9 minutes from call to first read.

Each step shows its target minute, counted from the first page. Until August 19, the provider pages you.

Step	Who calls whom	Number	Say, and bring
1 (0)	Owen: Takes the page	315-555-0101	Open the log. Write the time.
2 (10)	Owen: Imani, Mireille	315-555-0102	What you saw. Mireille then leads.
3 (15)	Mireille: Vantalect	The Incident Line	Page first, paper second; call-back in 30 minutes. Bring the time and what was seen.
4 (20)	Mireille: Harold	315-555-0104	What, where, since when.
5 (30)	Harold: Diane	212-555-0141	Ask her to sign the activation.
6 (40)	Diane: Signs it	212-555-0141	She quotes the reference and emails it.
7 (45)	Harold: Broker	800-555-0160	Discovery time as recorded. Bring the declarations page.
8 (50)	Mireille: Runs it	Console	One call. Tell Vantalect the hold is off.
9 (55)	Imani: AWS Support	Console	Bring account IDs, Region, the alert.
10 (60)	Harold: FBI office	Counsel's file	Only if counsel advises. Bring counsel's summary.

Activation, in four steps

1. **Counsel signs** the pre-agreed statement of work, quotes `WF-IR-SOW-2026-01`, and emails Mireille Danvers and Vantalect. Our hands-on commitment starts there.
2. **One command.** Mireille Danvers (or Imani Castell) runs `wf-ir-activate --reference WF-IR-SOW-2026-01 --approver ciso`. It removes the hold in all 22 accounts.
3. **Vantalect reads.** Charles assumes the role from an MFA session of his named IAM user, with the external ID and source identity.
4. **We propose, you approve.** Mireille approves each step by name; Imani attaches it.

Who may release the hold. Mireille Danvers or Imani Castell. If neither is reachable, the hold stays on and the bank follows its internal escalation procedure; this sheet names no third approver. The backups in the table below are for reaching people, not for releasing the hold.

Who is who

The bank's people and counsel. Every number is fictional; addresses are in the bank's contact list.

Person	Role	Phone	Backup
Owen Tribble	On call	315-555-0101	Imani
Imani Castell	Technical lead	315-555-0102	Owen
Mireille Danvers	Incident lead	315-555-0103	Imani
Harold Penwick	Calls counsel	315-555-0104	Mireille
Anand Sethuraman	Risk	315-555-0105	Harold
Colette Marsh	BSA	315-555-0106	Anand
Gregory Ashworth	CEO	315-555-0107	Mireille
Rafael Quintero	Account owner	315-555-0108	Imani
Lucía Brandt	Account owner	315-555-0109	Rafael
Diane Whitcombe	Counsel (firm line 212-555-0140)	212-555-0141	The firm

Vantalect: Charles Sieg. Vantalect gives each Retainer holder its Incident Line in writing at signature. It publishes no incident phone number or mailbox, and the Retainer is not yet offered.
No second contact. If no one answers, the Incident Lead proceeds with the stored containment policies and tells counsel. Planned absences: written notice, then a covering responder or a credit; illness and travel are inside the commitments.

Other parties. Real agencies and services have no number on this sheet.

Other party	Number	When, and what to bring
Security service provider	866-555-0170	If its alert is how you learned. The finding ID.
Carrier claims line	800-555-0161	Through the broker, or direct if the broker cannot be reached. The declarations page and discovery time.
AWS Security IR	Service console	Only where the bank subscribes. The bank has not decided to. Account IDs, Region, the alert.
FDIC, Federal Reserve, NYDFS	Counsel's file	Only as counsel and the bank decide. What counsel says.

Documents and the guardrail pack

- **Pre-agreed incident statement of work.** Counsel's system; legal folder copy. Held by Diane.
- **Insurance declarations page, broker's notice form.** The GC's binder. Held by Harold.
- **The activation command and the hold.** The bank's policy repository. Held by Imani.
- **The break-glass credential.** Sealed; location on the CISO's office list, never here. Held by Mireille.

The guardrail pack is in the bank's policy repository, and a sealed copy is in the evidence account's bucket: account `wf-ir-forensics` (`584729107701`), bucket `wf-ir-evidence`, prefix `guardrail-pack/`, in organization `o-wrnfld4x7q`. The policies are stored detached, so stage 1 is attaching. Files: `containment-scp.json`, `outside-principal-rcp.json`, `vault-deny-all-scp.json`, `hold-scp.json`, `SHA256SUMS`.

The first-hour checklist

1. Write the time of the first alert and who saw it. Turn nothing off, reboot nothing, delete nothing.
2. Do not contact or pay the attacker. The CISO names one spokesperson.
3. Page Vantalect first. Get counsel to sign, run the command, and confirm Vantalect can read.
4. Call the broker within the hour with the discovery time as recorded.
5. Confirm the trail is logging and the evidence bucket is untouched. Attach stage 1 only when the approver says yes; write the time.

6. Park questions about regulators, the board, and customers with counsel. The first situation report is due within 12 hours of the activation.

This sheet does not cover what the bank must report, to whom, or when; ask counsel. Review after the tabletop and after any change of people or numbers.

Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

© 2026 Vantalect, LLC. Sample deliverable; Wrenfield Bancorp, Inc. is fictional.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. MITRE ATT&CK is a registered trademark of The MITRE Corporation. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Other product names are trademarks of their owners. Vantalect is not affiliated with or endorsed by any of them. Wrenfield Bancorp, Inc. is fictional.