

Vantalect

SAMPLE ENGAGEMENT REPORTS

Sample Engagement Reports

Reading guide to the 22 reports · prepared for Wrenfield Bancorp, Inc.

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

September 15, 2026 · One breach, three engagements: the Response, the Investigation and the Recovery, and the Retainer

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.

Contents

What these reports are 2

The client 3

What happened 4

The three engagements 6

- The Response 6
- The Investigation and the Recovery 7
- The Retainer 8

Where to start 9

What is real and what is simulated 10

What these reports are

These are the 22 reports a bank receives from three Vantalect engagements that follow one ransomware incident from its first night to its first quarter of readiness: the Response (AWS Incident Response), the Investigation and the Recovery (AWS Breach Forensics & Recovery), and the Retainer (AWS Incident Response Retainer). They are samples. **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.** The legal citations, deadlines, and case summaries in the reports are illustrative as of the sample date, unverified in part, not legal advice, and not a template. The bank's domain is `wrenfield.example`.

Wrenfield is the fifth sample client, and the only one whose reports begin in an emergency. The first four clients bought planned work: a security audit, a cloud foundation, a Well-Architected review, a cost optimization. Wrenfield called at 00:41 on a holiday Saturday, through its outside counsel, because someone had encrypted its loan files. The 22 reports run 487 pages.

- **The track decides who reads.** Every report carries a distribution line under its title: **Counsel only** (11 reports, prepared at the direction of counsel), **Operational** (9 reports, for the bank's incident and platform teams), or **Releasable** (2 reports, facts that counsel may share with regulators, insurers, auditors, and peers once counsel clears them). Counsel decides what leaves the bank. The situation reports (Report ir-1) are Operational, for the bank's incident team as well as counsel. Three reports carry a part for a narrower audience than the report's track. Report 5 of the Investigation (Root Cause and Vulnerable Infrastructure) has an operational appendix for the bank's platform team. The Report 7 clock worksheets (Notification-Clock Worksheets) and the Notification-Clock Worksheets (Interim) have a suspicious activity report (SAR) annex for counsel and the BSA officer only. The text of the SAR confidentiality rule, 31 CFR 1020.320(e)(1)(i), names a bank's directors, officers, employees, and agents (read at the eCFR on October 28, 2026); whether Vantalect is an agent is for counsel to decide.
- **The numbers agree.** One generator builds the estate, the attack, and the response from a fixed scenario of 1,709 recorded API calls. A time in one report is the same time in every report, and a count is the same count. Reports dated earlier state only what was known on their date.
- **The reports do not give legal advice.** The legal memo and the notification-clock worksheets organize facts and compute deadlines from the times the bank recorded. The bank and its counsel decide what applies, what was material, and when notice is due. Vantalect makes no legal determination.
- **Hours are totals.** Where a report states consultant hours, it states what the engagement used in total.

The client

Wrenfield Bancorp, Inc., headquartered in Syracuse, New York, is a listed holding company. Wrenfield Bank is a New York-chartered commercial bank, not a Federal Reserve member, with 61 branches across central and western New York, $7.4 billion in assets, and 1,240 employees. Its federal regulator is the FDIC, the holding company's is the Federal Reserve, and its state regulator is NYDFS. Core banking runs at a vendor's service bureau, outside AWS. Since 2021 AWS has run its loan origination platform, its document imaging archive (loan files, check images, and signature cards), its data lake, its digital account-opening and online-banking middleware, and its treasury management portal, in 20 accounts in one AWS Organization.

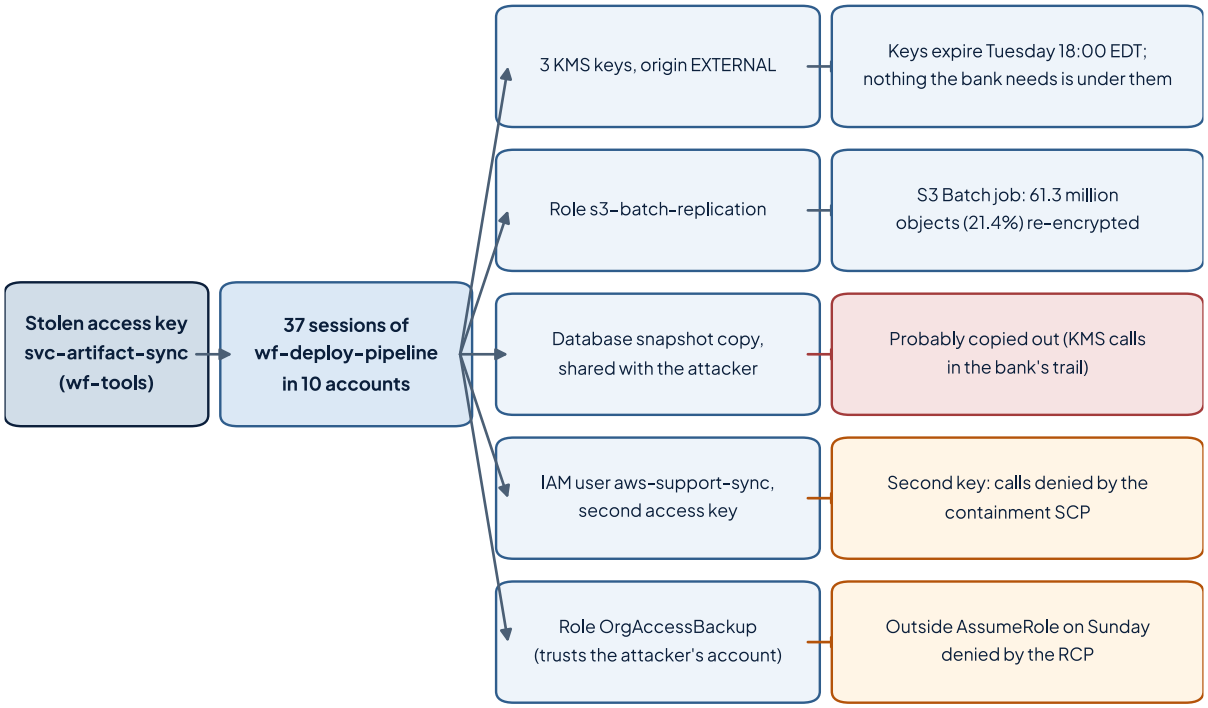
The people who appear in the reports. Every name except Vantalect's is invented.

Person	Title	Role in the case
Mireille Danvers	Chief Information Security Officer	Sponsor (bank side)
Diane Whitcombe	Partner, Tessaly & Brook LLP (outside counsel)	Contracting party for incidents
Harold Penwick	General Counsel	Consulted
Gregory Ashworth	President and Chief Executive Officer	Consulted
Imani Castell	Cloud Platform Lead	Lead
Owen Tribble	Senior Cloud Engineer	On call, July 3
Lucía Brandt	Head of Lending Operations	Workload owner
Rafael Quintero	Chief Information Officer	Workload owner
Anand Sethuraman	Chief Risk Officer	Risk
Colette Marsh	BSA/AML Officer	BSA officer (suspicious activity reports)
Charles Sieg	Vantalect	Author of all 22 reports

What happened

An attacker used one stolen access key to reach production, re-encrypted 61.3 million of the imaging archive's 286 million objects under keys only the attacker held, and set those keys to expire at the ransom deadline. The bank restored from its own copies before the keys expired, paid nothing, and closed the door.

The key belonged to the IAM user `svc-artifact-sync`. It was taken from a contractor's personal laptop, was first used on Monday, June 29, 03:14 EDT, and had never been rotated. For 4 days, 17 hours, 50 minutes the attacker only read and tested access. On Friday, July 3, 21:04 EDT, the evening of the Independence Day federal holiday, the attacker assumed `wf-deploy-pipeline` in production, created 3 KMS keys with imported key material set to expire on Tuesday, July 7 UTC, started an S3 Batch Operations job over the imaging archive, deleted snapshots, and left a ransom note demanding $14.5 million in cryptocurrency. The first containment control, a service control policy, went on 4 hours 18 minutes after the first write.



The attacker's credential chain, the things it made, and the calls that were denied.

The dates the reports share.

Date	What happened
Monday, June 29	First use of the stolen key, read-only
Friday, July 3	First write in production; the ransom note at 23:30
Saturday, July 4	Emergency activation signed at 00:52 EDT; the containment policy attached at 01:22 EDT
Saturday, July 4	The bank's determination meeting; notices to the FDIC and the Federal Reserve
Sunday, July 5	NYDFS notified
Tuesday, July 7	The imported key material expires at 18:00 EDT; nothing the bank needs is under it
Thursday, July 9	Containment declared in writing; the Response ends
Monday, July 13 to Friday, August 7	The Investigation and the Recovery, four weeks; the readout on Friday, July 24
Monday, August 10	The Retainer begins, for one year

The three engagements

Wrenfield signed three engagements in the order the incident demanded them. The Response ran from July 4 to July 9, 56 hours in total, at $675 an hour ($37,800), authorized in the first hour at $16,200. The Investigation and the Recovery ran four weeks from July 13 to August 7: 104 of 110 included hours used, for $41,900 after a $8,100 credit for 18 Response hours. The Retainer began August 10 for one year at $36,000, with 48 readiness hours used and 40 prepaid readiness hours untouched at the sample's end. In all, Wrenfield paid $115,700.

The Response

The Response contains the incident while evidence is preserved. It is delivered while the incident is running, so it is short, fast, and built for counsel to read at 3 AM.

AWS Incident Response: the reports, who may read them, and when each was dated.

Report	Distribution	Dated	Pages	What it delivers
Operational Situation Reports	Operational	Jul 9	34	What was known, what was being done, and what came next, report by report on the fixed rhythm, for the bank's incident team; legal items go to counsel in the clock worksheet.
Containment and Eradication Actions	Operational	Jul 9	46	Every action taken, who approved it, what it changed, what was preserved first, and how to undo it.
Executive Brief at Containment	Counsel only	Jul 9	5	One page the CEO and board can read once counsel forwards it: what happened, what is protected, what is still unknown, and what decisions are theirs.
Notification-Clock Worksheets (Interim)	Counsel only	Jul 9	27	The deadlines that may run from the client's own determinations, computed from the times the client entered, with the facts each needs.
Chain-of-Custody Log (at Containment)	Counsel only	Jul 9	34	Every evidence item from collection to storage, hashed, so counsel can authenticate it.

The Investigation and the Recovery

The Investigation answers how the attacker got in, what they touched, and whether they are out. The Recovery, which delivers all twelve reports, adds eradication, root-cause closure, and a closure sweep that gates the hand-over. The Investigation alone delivers reports 1 through 7 and the final custody log.

AWS Breach Forensics & Recovery: the reports, who may read them, and when each was dated.

Report	Distribution	Dated	Pages	What it delivers
Estate Map and Evidence Preservation	Counsel only	Jul 17	33	The organization as it stood, every log source and its gaps, and what was preserved, so every later claim has a source.
Attack Narrative and Timeline	Counsel only	Jul 24	43	What the attacker did, in order, minute by minute, from first access to the last attempt, with each step's evidence.
Indicators of Compromise	Releasable	Jul 24	25	Every indicator in one table and in machine-readable form, for the client's detections, its peers, and law enforcement, once counsel clears it.

Report	Distribution	Dated	Pages	What it delivers
Executive Brief	Counsel only	Jul 24	9	The Investigation's answer for the board: how they got in, what they touched, whether they are out, and what closes the door.
Compromise Inventory	Counsel only	Jul 24	16	Every principal, credential, resource, and data set the attacker used, created, changed, read, or copied, with confidence.
Root Cause and Vulnerable Infrastructure	Counsel only	Jul 24	19	Why the attack worked at each step, and what else in the estate would have let it work; an operational appendix holds the control gaps and the fix plan.
Legal and Regulatory Considerations: Draft for Counsel	Counsel only	Jul 24	32	The facts counsel needs, organized by the regimes counsel may want to consider; a draft for counsel, not legal advice.
Notification-Clock Worksheets	Counsel only	Jul 24	27	The interim worksheets brought up to the Investigation's facts.
Eradication and Root-Cause Closure	Operational	Jul 31	19	Every inventory item removed or isolated and every critical root cause fixed as code, with its pull request.
Closure Sweep	Operational	Aug 7	16	The gate: week one against week four, the same method, and seven days of watch.
Factual Summary for Regulators, Insurers, and Auditors	Releasable	Aug 7	6	Facts only, no analysis or opinion, for counsel to release.
Chain-of-Custody Log (Final)	Counsel only	Aug 7	42	The full custody record at the close, with the destruction certificate for Vantalect's working copies.

The Retainer

The Retainer makes the next incident cheaper and faster: an activation role the bank can invoke in one call, a log-readiness check, a readiness readout, a tabletop exercise, and a call sheet.

AWS Incident Response Retainer: the reports, who may read them, and when each was dated.

Report	Distribution	Dated	Pages	What it delivers
Activation Role and Drill	Operational	Aug 12	15	The role deployed, the drill run, and the measured minutes from activation to first read.
Log-Readiness Check	Operational	Aug 21	12	Whether the evidence the next investigation needs will exist, and what each gap costs to close.
Readiness Readout	Operational	Aug 28	11	What the client is ready for now, what is still exposed, and the commitments in force.
Tabletop Exercise After-Action Report	Operational	Sep 15	11	What the team did with a realistic scenario, where it slowed down, and what changes.
Activation Call Sheet	Operational	Aug 14	5	Who calls whom, in what order, with which numbers and documents, at 1 AM on a holiday.

Where to start

Read by role. Each path below starts with the shortest document that answers your first question.

- **The chief executive officer and the board.** You need the answer, what is still unknown, and which decisions are yours. Executive Brief at Containment; Executive Brief; Factual Summary for Regulators, Insurers, and Auditors.
- **Outside counsel and the general counsel.** You decide notification, privilege, and release, and you need the facts organized by regime, the clocks, and the evidence. Notification-Clock Worksheets (Interim); Legal and Regulatory Considerations: Draft for Counsel; Notification-Clock Worksheets; Chain-of-Custody Log (at Containment); Chain-of-Custody Log (Final); Factual Summary for Regulators, Insurers, and Auditors.
- **The chief information security officer and the cloud platform lead.** You own the fix, and you need what happened, why it worked, and how the door was closed. Attack Narrative and Timeline; Root Cause and Vulnerable Infrastructure; Compromise Inventory; Eradication and Root-Cause Closure; Closure Sweep.
- **An incident responder on the bank's team or a peer's.** You need the actions, the indicators, and the call sheet. Containment and Eradication Actions; Indicators of Compromise; Activation Role and Drill; Activation Call Sheet.
- **The bank's chief risk officer and its BSA officer.** You need the clocks, the compromise inventory, and what is still exposed. Notification-Clock Worksheets (Interim); Notification-Clock Worksheets; Compromise Inventory; Readiness Readout.

What is real and what is simulated

The method is real; the bank is not. The legal citations, deadlines, and case summaries are illustrative as of the sample date, unverified in part, not legal advice, and not a template; counsel must check any of them before relying on it. The reports are made by the same generator and checks as Vantalect's other samples: the same layout, the same accessibility checks, the same rule that a figure is never typed by hand. The AWS service behavior, the API names, the event shapes, and the controls (service control policies, resource control policies, S3 Object Lock, AWS Backup Vault Lock, KMS key material expiry) are real. The company, its people, its accounts, its figures, the attacker, and every address are invented, and the attacker's addresses come from ranges reserved for documentation. Pursuit, Vantalect's tracker, reconstructs the attacker's sessions from the recorded calls in the scenario, and the figures in these reports that come from it are drawn from its output.

The reports say what they do not know. The imaging archive's reads were not logged, so the reports never claim the archive was or was not read. Whether data was copied out is stated as probable in the counsel-track reports and never as confirmed. Attribution is consistent with, never proof of, a financially motivated actor, and no real group is named.

What the label does and does not do

Counsel-track reports carry "Privileged and confidential. Prepared at the direction of counsel." The label alone protects nothing. Whether privilege applies depends on how the work was commissioned and handled, and counsel decides.

© 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.