

Vantalect

AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Legal and Regulatory Considerations: Draft for Counsel

DISTRIBUTION: COUNSEL ONLY

Week 2 of 4: Trace · prepared for Wrenfield Bancorp, Inc.

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

July 24, 2026 · AWS Breach Forensics & Recovery: The Investigation and the Recovery (four weeks)

SAMPLE DELIVERABLE

Privileged and confidential. Prepared at the direction of counsel. Sample. Wrenfield is fictional.

Draft for counsel's review. Not legal advice. Vantalect makes no legal determination.

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

About this memo **3**

The facts counsel needs **4**

The incident in brief 4

Data types and record counts by state of residence 4

Access versus acquisition 5

The dates the bank recorded 7

Systems disrupted and for how long 9

Law-enforcement contact 10

The regimes counsel may want to consider **10**

Bank regulators 12

New York 16

Other states 18

Securities disclosure 19

Suspicious activity reporting 20

Other federal and sector rules 21

Ransom and sanctions **22**

Preservation and litigation hold **24**

What was preserved 24

Recovery copies, not preserved evidence 25

What was not logged or was lost 26

What counsel may want to consider 26

Privilege and distribution 26

Contracts that may carry notice duties **27**

The questions only counsel can answer **29**

Questions by regime 29

Questions across regimes 30

Notice **32**

About this memo

This is a draft for counsel's review. It gathers the facts Wrenfield's counsel needs and sets them against the regimes counsel may want to consider, and it reaches no legal conclusion. It is dated Friday, July 24, 2026. It is written for Diane Whitcombe of Tessaly & Brook LLP, and it goes to counsel only. We are Vantalect. We supply facts and compute deadlines from times the bank entered. The bank and counsel decide whether any regime applies, whether anything is material, what the discovery date is, whether any notice is due, and whether privilege applies.

Distribution and privilege

Privileged and confidential. Prepared at the direction of counsel. The label does not protect a document by itself: privilege depends on how and why the work was commissioned, and counsel decides whether it applies. Vantalect makes no determination about privilege. This memo is a draft. Drafts and comments may be discoverable, and counsel decides whether a written memo is needed at all. It should not be copied into the facts-only summary that counsel may later release.

What it does not hold. It does not say that any regime applies, that anything was or was not material, that any notice is or was due, or that any notice was timely. It does not tell the bank what to do. It does not cover tax, employment, securities disclosure beyond Form 8-K Item 1.05, or any non-United States law. It has not seen the bank's contracts, insurance policies, or the notices the bank sent. It holds no record of any suspicious activity report review, filing, or non-filing, and it will not.

Where the legal texts come from. Each regime section gives the citation and the status of its text, and the ransom and preservation sections cite the advisories and rules they rely on. Where a point could not be checked against the official text, it is stated as a question for counsel and not as a rule. Counsel should check every quotation and citation against the current official text before relying on it. **Publication note.** The source checks named in the status lines were made in October 2026, when this sample was published. The bank did not have those readings on July 24.

How the memo and the clock worksheets fit. The Notification-Clock Worksheets compute each deadline from the times the bank entered. This memo repeats the recorded times where they matter and does not replace them.

The facts counsel needs

The facts below are what we had on July 24, with our confidence stated beside each. Times are Eastern Daylight Time. Where we write "probable" or "unknown" we mean exactly that.

The incident in brief

An attacker used a long-lived access key for the bank's service user `svc-artifact-sync`, first seen at 03:14 EDT on Monday, June 29, 2026. After 4 days, 17 hours, 50 minutes of read-only exploration, the first write-capable attacker session in production began at 21:04 EDT on Friday, July 3. The attacker created 3 KMS keys with imported key material set to expire at 18:00 EDT on Tuesday, July 7, re-encrypted 61,300,000 objects in the imaging archive under those keys, deleted backups, left a ransom note in three buckets, and shared a copy of the loan origination database with an outside account. The bank removed that share at 02:08:20 EDT on Saturday, July 4, after 137 minutes, and finished closing the path at 02:10:30 EDT. The bank and Vantalect contained the rest, and the bank restored the affected data and backups, except one legacy account trail that was deleted. The bank's containment declaration is recorded at 09:00 EDT on Thursday, July 9.

Data types and record counts by state of residence

The loan origination system holds 412,317 applicant records, and the counts by state come from a query the bank ran on its loan system. Vantalect does not attest to them. Per the bank's description, the records are names, Social Security numbers, dates of birth, and income.

Applicant records by state of residence, from the bank's own count.

State of residence	Applicant records
New York	389,904
Pennsylvania	15,077
Other states	7,336
Total	412,317

Where the counts come from. The bank's analyst ran the query on the loan origination system of record, `wf-los-prod`, and gave the result to counsel. The Chain of Custody Log holds the record of who ran it, on which system, and when. Our role does not let us read stored data, and we did not

collect the data in the database snapshot. We did not run the query, we have not read the records, and we do not attest to the counts. They drive every state notice, so counsel may want its own check of them.

The imaging archive. The bank's estate profile says the archive, `wf-imaging-archive-prod`, holds loan files, check images, and signature cards: 286,000,000 objects and 412 TB. We have not opened any object, so we do not say which data elements appear in them. Check images and signature cards are the kind of document that may show a name with an account number. Whether any object does is for the bank and counsel. The 412,317 above is a count of database records, not of archive objects.

Two limits apply. The counts hold no split of the other states, and we have not reviewed the contents of the loan files in the imaging archive. Whether the archive holds records that matter to any statute is a question for the bank's lending team and counsel.

Access versus acquisition

The copy-out of the database snapshot is probable, with high confidence. It is not confirmed. The table sets out each place data was reachable, what the record shows, and how sure we are. We never saw data leave the bank's accounts. We infer the copy from key use that is logged. For the imaging archive, we state what the attacker's job did and under whose credentials, and we do not say whether that is access.

The record on access and acquisition, by place.

Place	What the record shows	Status
Loan origination database snapshot	The attacker made a snapshot at 21:22 EDT on July 3, copied it under a KMS key it had created in the bank's lending account, and shared the copy with account `777788889999` at 23:51:12 EDT (`EV-00520`). The bank removed the share at 02:08:20 EDT on July 4 (`EV-00632`), 137 minutes after it was added. The bank's trail logged 7 KMS calls on that key from the outside account in the copy-out burst, and 7 outside-account calls through Saturday, July 4. They are listed below.	Copy-out probable, high confidence
Imaging archive	The attacker's S3 Batch Operations job (`EV-00393`, created at 21:41 EDT on July 3 in `wf-prod-imaging` by an attacker session of the `wf-deploy-pipeline` role at `203.0.113.47`) ran as the role `s3-batch-replication`. For each object, S3 copied the object onto itself under the attacker's imaging key, with the metadata kept. That is a server-side operation on each object's content, run under the attacker's control and the job role's credentials. It ran 227 minutes and reached 61,300,000 of 286,000,000 objects (21.4%) before the bank canceled it at 01:28:05 EDT on July 4. The job's report was disabled, so there is no completion report. Reads were not logged.	Reads unknown
Data lake bucket	214 copy attempts with customer-supplied keys were all denied within 40 seconds.	Denied, no change
Lending documents bucket	A ransom note was found by listing. The bucket has no data events, so reads and writes are not logged.	Reads unknown
Hosts and applications	No host access to any instance was found. The loan platform's application and load-balancer logs show no attacker traffic.	None found

The outside-account KMS calls on the lending attacker key are these, from the bank's organization trail. The first seven are the copy-out burst.

The outside-account KMS calls on the lending attacker key, in time order. The first CreateGrant row covers two calls.

Time (EDT)	Call	What the record shows
00:06:09 EDT	`CreateGrant`	A grant to the role `exfil-runner` in the outside account, and a second grant at 00:06:37 to the RDS service with `exfil-runner` as the retiring principal. `EV-00522`
00:06:21 EDT	`DescribeKey`	The key described by the same session. `EV-00523`
00:07:02 EDT	`ReEncrypt`	Ciphertext re-encrypted from the lending key to a key in the outside account, invoked by RDS. `EV-00525`
00:28:14 EDT	`Decrypt`	Decrypt invoked by RDS, with the snapshot as the encryption context. `EV-00528`
00:50:48 EDT	`Decrypt`	Decrypt invoked by RDS, with the snapshot as the encryption context. `EV-00530`
00:51:06 EDT	`RetireGrant`	The RDS grant retired. This is the last call of the burst. `EV-00531`

Statutes differ in whether they turn on access, acquisition, or both, and in how they treat encrypted data. The snapshot copy was encrypted under a key the attacker created, and the attacker's account held a grant on that key while the share was open. Counsel decides which wording applies and what our evidence supports. Whether the in-place re-encryption of the imaging objects is access to, or acquisition of, the data in them under any text is for counsel.

The dates the bank recorded

These are the recorded events, each with who recorded it and from what source. We do not choose among them, and we do not say which is the discovery date. The discovery date, the date of any determination, and whether any regime applies are for the bank and counsel.

Recorded events up to the bank's determination, in time order, with who recorded each and from what source.

Date and time (EDT)	What was recorded	Recorded by, and source
Monday, June 29, 03:14 EDT	First use of the stolen key, read-only	Vantalect, from the organization trail
Friday, July 3, 21:04 EDT	First write-capable attacker session in production	Vantalect, from the organization trail
Friday, July 3, 22:44 EDT	GuardDuty finding, forwarded to the managed security service provider	The provider's alert queue and the bank's logs
Friday, July 3, 23:18 EDT	The provider pages the bank's on-call engineer	The provider's page record and the bank
Saturday, July 4, 00:05 EDT	The on-call engineer confirms the ransom note	The bank
Saturday, July 4, 00:52 EDT	Emergency activation signed under counsel's letter	Counsel
Saturday, July 4, 01:22 EDT	Containment policy attached	The bank, from the organization trail
Saturday, July 4, 02:08:20 EDT	The share of the database snapshot with account 777788889999 removed, 137 minutes after it was added. Three key policies changed at 02:09, and the attacker's grant revoked at 02:10:30 EDT	The bank, from the organization trail
Saturday, July 4, 06:00 EDT	Report to the FBI field office	The bank
Saturday, July 4, 09:40 EDT	IC3 complaint filed	The bank

Recorded events from the bank's determination, in time order, with who recorded each and from what source.

Date and time (EDT)	What was recorded	Recorded by, and source
Saturday, July 4, 10:00 EDT	The bank's determination meeting	The bank, with counsel
Saturday, July 4, 14:30 EDT	FDIC notified	The bank
Saturday, July 4, 14:45 EDT	Federal Reserve notified	The bank
Sunday, July 5, 11:15 EDT	NYDFS notified	The bank
Thursday, July 9, 09:00 EDT	Containment declared in writing	The bank
Tuesday, July 14, 2026	Materiality determination	The bank and counsel
Friday, July 17, 2026	Form 8-K filed	The bank
Saturday, July 4, 2026	The date entered as the discovery date in the Notification-Clock Worksheets	The bank and counsel, as their entry

Systems disrupted and for how long

Loan origination was offline for 110 hours 10 minutes, by the bank's own decision to freeze its state. The other disruption was to data and backups, and the bank restored them. One legacy account trail's configuration was deleted and not recreated; files it had delivered remain unless separately deleted.

Systems disrupted, how, and how long.

System	What happened	Measure
Loan origination	Taken offline by the bank at 01:50 EDT on July 4 and returned at 16:00 EDT on Wednesday, July 8	110 hours 10 minutes; 1,912 applications queued
Imaging archive	Objects re-encrypted under attacker keys, then rewritten by the bank under its own key in 31 sequential jobs by 12:40 EDT on July 7	61,300,000 objects; 0 current under attacker keys at 14:00 EDT
EBS snapshots	Deleted, then restored from the Recycle Bin at 07:40 EDT on July 4	46 deleted; 46 restored
Database snapshots	The month-end manual snapshots were deleted and restored from the backup account	9 deleted; 9 restored
Legacy account trail	Deleted by the attacker. The organization trail kept recording	One trail

We have not measured how long any archive object was unreadable, and we have no finding on how long any other service was degraded.

Law-enforcement contact

Harold Penwick reported to the FBI field office at 06:00 EDT on July 4, and the bank filed an IC3 complaint at 09:40 EDT. We have no record of contact with any other agency, and no record of a written request from any agency that a notice be delayed. Counsel should confirm both.

The regimes counsel may want to consider

We list sixteen regimes, and we say for none of them that it applies. The overview gives each text's citation and how far we could read it. The sections after it give the text, the recorded times, and the facts relevant to each. The questions for the regimes new or changed in this edition are in Questions by regime. CL-8 and CL-9 are listed only so counsel can rule them out. X-6, the Interagency Guidance, is guidance with no deadline in days, so no deadline is computed for it.

Bank regulators and New York. The IDs match the Notification-Clock Worksheets.

ID	Regime	Citation	Source status
CL-1	FDIC computer-security incident notification	12 CFR 304.23	Rule text quoted
CL-2	Federal Reserve notification (holding company)	12 CFR 225.300 to 225.303 (Subpart N)	Rule text quoted
X-6	Interagency Guidance on customer information incidents (GLBA Section 501(b))	Supplement A to Appendix B to 12 CFR Part 364 (FDIC, for the bank); Supplement A to Appendix F to 12 CFR Part 225 (Federal Reserve, for the holding company); Supplement A to Appendix D-2 to 12 CFR Part 208 (Federal Reserve, for a state member bank)	Rule text quoted
CL-8	OCC computer-security incident notification	12 CFR 53.3	Rule text quoted
X-2	Bank service provider rules	12 CFR 53.4 and 12 CFR 304.24	Rule text quoted
CL-3	NYDFS cybersecurity incident notice	23 NYCRR 500.17(a)	Rule text quoted
CL-7	NYDFS extortion payment notices	23 NYCRR 500.17(c)	Rule text quoted
CL-6	New York GBL 899-aa	N.Y. Gen. Bus. Law 899-aa	Secondary source

Other states, securities, suspicious activity reports, other federal rules, and sanctions.

ID	Regime	Citation	Source status
X-3	Pennsylvania breach notification statute	Breach of Personal Information Notification Act, Act 94 of 2005, as amended by Act 33 of 2024 (P.L. 427, No. 33)	Rule text quoted
X-4	Other state breach statutes	statutes to be identified by counsel	Secondary source
CL-4	SEC current report on a cybersecurity incident	Form 8-K, Item 1.05	Text as we have it
CL-5	FinCEN suspicious activity report	31 CFR 1020.320(b)(3) and (e)	Rule text quoted
CL-9	FTC Safeguards Rule notice	16 CFR 314.4(j)	Rule text quoted
X-1	HIPAA breach notification	45 CFR 164.404	Rule text quoted
CL-10	CIRCIA covered-incident reporting	6 U.S.C. 681b	Rule text quoted
X-5	OFAC sanctions considerations	OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021)	Rule text quoted

Bank regulators

FDIC computer-security incident notification (CL-1)

What the text says. The FDIC's rule at 12 CFR 304.23 sets a 36-hour period that runs from the time the banking organization determines that a notification incident has occurred. The OCC's parallel text at 12 CFR 53.3 reads "no later than 36 hours after the banking organization determines that a notification incident has occurred." At 12 CFR 53.2 the OCC defines a computer-security incident as "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system," and a notification incident as one that has materially disrupted or degraded, or is reasonably likely to, core operations, a business line, or United States financial stability. Counsel should confirm the FDIC's own definitions, which we treated as parallel.

Citation and source status. 12 CFR 304.23. Quoted from the rule's text. Counsel to confirm the current text.

Recorded times and the computed deadline. The bank recorded its trigger as Saturday, July 4, 10:00 EDT, and the computed deadline is Sunday, July 5, 22:00 EDT. The bank recorded the notice at 14:30 EDT on Saturday, July 4.

Facts relevant to it.

- The bank recorded its determination, in the rules' own terms, that a notification incident and a cybersecurity incident had occurred. That determination is the bank's, and we make no finding on it.
- Loan origination was offline for 110 hours 10 minutes. The imaging archive and the backups were disrupted as in Systems disrupted and for how long.
- We make no finding on the rule's definitions of a computer-security incident or a notification incident.

Federal Reserve notification (holding company) (CL-2)

What the text says. The Federal Reserve's computer-security incident notification rule is 12 CFR Part 225, Subpart N (225.300 to 225.303). It applies to bank holding companies, savings and loan holding companies, and state member banks. Section 225.302 calls for notice to the Board-designated point of contact "as soon as possible and no later than 36 hours after" the banking organization determines that a notification incident has occurred. The period runs from each banking organization's own determination, so the bank's determination is not automatically the holding company's. Section 225.301 defines a notification incident. The FDIC's counterpart for the state nonmember bank is 12 CFR 304.23, listed as CL-1. Whether the event is a notification incident is for counsel.

Citation and source status. 12 CFR 225.300 to 225.303 (Subpart N). Text of 225.302 checked at the Federal Reserve Regulatory Service for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current text.

Recorded times and the computed deadline. The holding company's own determination is not recorded here. As an illustration only, if it also determined at the bank's recorded time of Saturday, July 4, 10:00 EDT, the period would end Sunday, July 5, 22:00 EDT. The bank recorded the notice at 14:45 EDT on Saturday, July 4.

Facts relevant to it.

- The holding company is Wrenfield Bancorp, Inc..
- We do not know whether the holding company recorded a separate determination.

Interagency Guidance on customer information incidents (GLBA Section 501(b)) (X-6)

What the text says. The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice implements Section 501(b) of the Gramm-Leach-Bliley Act. The FDIC form is Supplement A to Appendix B to 12 CFR Part 364, which applies to insured state nonmember banks (12 CFR 364.101(b) points to the Appendix). The holding-company version is Supplement A to Appendix F to 12 CFR Part 225, and the state-member-bank version is Supplement A to Appendix D-2 to 12 CFR Part 208. The guidance says a response program should include notifying the 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." After a reasonable investigation to "promptly determine the likelihood that the information has been or will be misused," the institution should notify the affected customer "as soon as possible" if misuse "has occurred or is reasonably possible." Notice may be delayed if an appropriate law enforcement agency determines that notice would interfere with a criminal investigation and gives a written request. If the institution cannot tell which customers in a group of files were accessed and misuse is reasonably possible, it should notify all customers in the group. Sensitive customer information is a name, address, or telephone number together with a Social Security number, driver's license number, account number, credit or debit card number, or a PIN or password that would permit access to the account, and any combination of components that would allow someone to log on to or access the account. This is guidance ("should"), and it sets no deadline in days, so we compute nothing for it.

Citation and source status. Supplement A to Appendix B to 12 CFR Part 364 (FDIC, for the bank); Supplement A to Appendix F to 12 CFR Part 225 (Federal Reserve, for the holding company); Supplement A to Appendix D-2 to 12 CFR Part 208 (Federal Reserve, for a state member bank). Appendix structure checked at the eCFR for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current text of each Supplement.

Recorded times and the computed deadline. None. The Interagency Guidance sets no deadline in days, and we compute nothing. The bank recorded notices to the FDIC at 14:30 EDT and to the Federal Reserve at 14:45 EDT on Saturday, July 4 (the notices recorded at CL-1 and CL-2). Whether those notices also serve the Guidance is for counsel.

Facts relevant to it.

- The applicant records number 412,317. Per the bank's description they hold names and Social Security numbers, with dates of birth and income. The counts by state (389,904 New York, 15,077 Pennsylvania, 7,336 other) come from a query the bank ran, and Vantalect does not attest to them.

- The imaging archive holds loan files, check images, and signature cards, which may show a name with an account number. We have not opened any object, so we do not say which customers' records were reached.
- The copy-out of the database snapshot is probable, with high confidence, and not confirmed. Object reads in the imaging archive are unknown. We have no record of a written request from a law-enforcement agency to delay customer notice.

OCC computer-security incident notification (CL-8)

What the text says. 12 CFR 53.3 is the OCC's notification rule for national banks, federal savings associations, and the other banking organizations the OCC supervises, and it sets the 36-hour period from a notification-incident determination. We list it only so that counsel can rule it out. The facts say the bank is a New York-chartered commercial bank and not a Federal Reserve member, with the FDIC as its federal regulator. The FDIC's counterpart is 12 CFR 304.23 (CL-1), and the Interagency Guidance is listed as X-6. Ruling it out is counsel's call.

Citation and source status. 12 CFR 53.3. Quoted from the rule's text. Counsel to confirm the current text.

Recorded times and the computed deadline. None. The bank has recorded no trigger for this rule, and we compute nothing.

Facts relevant to it.

- The bank is a New York-chartered commercial bank and not a Federal Reserve member. Its federal regulator is the FDIC.

Bank service provider rules (X-2)

What the text says. 12 CFR 53.4 (and 304.24 for the FDIC) calls for a bank service provider to notify at least one bank-designated point of contact "as soon as possible" once it determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to, covered services for four or more hours. The duty runs from a provider to a bank.

Citation and source status. 12 CFR 53.4 and 12 CFR 304.24. Quoted from the rule's text. Counsel to confirm the current text.

Recorded times and the computed deadline. None. This duty runs from a provider to a bank, and the bank has recorded no trigger.

Facts relevant to it.

- The managed security service provider received the GuardDuty finding at 22:44 EDT and paged the on-call engineer at 23:18 EDT, 34 minutes later.

- We found no outage of an AWS service or of a provider's system. The disruption was to the bank's own workloads.

New York

NYDFS cybersecurity incident notice (CL-3)

What the text says. 23 NYCRR 500.17(a)(1) calls for a covered entity to notify the superintendent electronically as promptly as possible, and in no event later than 72 hours after determining that a cybersecurity incident has occurred at the covered entity, its affiliates, or a third-party service provider. Section 500.1(g), as amended on November 1, 2023, defines a cybersecurity incident as a cybersecurity event at the covered entity, its affiliates, or a third-party service provider that (1) impacts the covered entity and requires it to notify any government body, self-regulatory agency, or other supervisory body; (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or (3) results in the deployment of ransomware within a material part of the covered entity's information systems. Section 500.17(a)(2) calls for the covered entity to promptly provide any information the superintendent requests, and it has a continuing obligation to update the superintendent with material changes or new information previously unavailable. Section 500.17(c), the extortion payment notice, is listed separately as CL-7. Whether the bank is a covered entity, and which prong applies, is for counsel.

Citation and source status. 23 NYCRR 500.17(a). Text of 500.1(g) and 500.17 checked in the Department of Financial Services' published amended Part 500 (November 1, 2023) for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current text.

Recorded times and the computed deadline. The bank recorded its trigger as Saturday, July 4, 10:00 EDT, and the computed deadline is Tuesday, July 7, 10:00 EDT. The bank recorded the notice at 11:15 EDT on Sunday, July 5.

Facts relevant to it.

- The bank recorded its determination that a cybersecurity incident had occurred, at the same time as in CL-1. That determination is the bank's, and we make no finding on it.
- The definition has more than one prong. The prong that names ransomware reads "deployment of ransomware within a material part of the covered entity's information systems." We list it and do not apply it. The facts the bank recorded that counsel may set against any prong are in the incident in brief, the systems disrupted, and the dates above.
- The definition and the notice duty reach events at affiliates and at third-party service providers. The one third party in our record is the managed security service provider, which received the GuardDuty finding. We found no event at it.

- The rule describes a continuing duty to update the superintendent. Facts that are new since July 5 are the state counts above, the rating of the copy-out as probable, and the finding that no host access was found.

NYDFS extortion payment notices (CL-7)

What the text says. 23 NYCRR 500.17(c) calls for notice of an extortion payment within 24 hours of the payment. Within 30 days of the payment it calls for a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations, including those of the Office of Foreign Assets Control. Both periods run from a payment, and no payment was made in this incident.

Citation and source status. 23 NYCRR 500.17(c). Text of 500.17(c) checked in the Department of Financial Services' published amended Part 500 for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current text.

Recorded times and the computed deadline. None. No payment was made, so nothing is computed.

Facts relevant to it.

- The demand was $14,500,000 in cryptocurrency by Tuesday, July 7, at 18:00 EDT. No payment was made.

New York GBL 899-aa (CL-6)

What the text says. N.Y. Gen. Bus. Law 899-aa, as amended in December 2024, concerns notice of a breach of the security of the system to affected New York residents, to state offices under subdivision 8(a), and to consumer reporting agencies under subdivision 8(b) when more than 5,000 New York residents are notified. Subdivision 2(b) concerns an entity that has already notified affected persons under a listed regime, including the Gramm-Leach-Bliley Act, HIPAA, and 23 NYCRR Part 500. The points counsel should confirm against the current official text are in the questions below.

Citation and source status. N.Y. Gen. Bus. Law 899-aa. The official text was not available for this edition's publication check. The description above and the questions below are for counsel to confirm against the current statute.

Recorded times and the computed deadline. The bank recorded its trigger as Saturday, July 4, 2026, and the computed deadline is Monday, August 3, 2026. The clock is open on July 24, with 10 days to the computed deadline.

Facts relevant to it.

- New York has 389,904 of the applicant records. Records are not residents notified, and the number of residents notified is for counsel.
- The data types are names, Social Security numbers, dates of birth, and income.
- The bank recorded its NYDFS notice (CL-3) at 11:15 EDT on Sunday, July 5. Subdivision 2(b) is read in the questions for CL-6: counsel decides whether the affected persons have already received a qualifying notice under a listed regime. The July 5 notice to DFS is a regulator notice, and we do not assume it meets that condition.
- The earliest attacker activity is Monday, June 29, 2026. The worksheet's trigger date is Saturday, July 4, 2026, the bank's entry. The discovery date is counsel's to set, and Vantalect does not say which date it is.
- The evidence on access and acquisition is in Access versus acquisition.

Other states

Pennsylvania breach notification statute (X-3)

What the text says. Act 33 of 2024 (Senate Bill 824, enacted June 28, 2024, effective 90 days later, on September 26, 2024) amends Act 94 of 2005. It adds subsection (c.1) to section 3: when notice of a breach must be given to more than 500 affected individuals in Pennsylvania, notice shall be made concurrently to the Office of Attorney General, with the organization name and location, the date of the breach, a summary, and estimated totals of affected individuals overall and in Pennsylvania. Subsection (c.2) exempts an entity subject to 40 Pa.C.S. Chapter 45 (insurance data security) from (c.1). Section 5 now calls for notice to the nationwide consumer reporting agencies when more than 500 persons are notified at one time (it was 1,000). New section 5.4 applies when an entity determines that a breach has occurred and reasonably believes that an individual's name, in combination with a Social Security number, bank account number, or driver's license or State ID number, has been accessed. An entity that provides notice under section 5 and meets those conditions then assumes the cost of access to one independent credit report for an individual who is not eligible for a free one, and of credit monitoring for 12 months, which it may satisfy by notifying the individual of the availability of monitoring at no cost, and it informs the individual of those services on notification. Whether the Act applies to the Pennsylvania residents among the records is for counsel.

Citation and source status. Breach of Personal Information Notification Act, Act 94 of 2005, as amended by Act 33 of 2024 (P.L. 427, No. 33). Text of Act 33 of 2024 checked at the Pennsylvania General Assembly site for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the whole Act 94 as amended, including section 3 and its exemptions.

Recorded times and the computed deadline. None. The bank has recorded no trigger and we compute nothing.

Facts relevant to it.

- Pennsylvania has 15,077 of the applicant records, each with a name and a Social Security number. Records are not residents notified.

Other state breach statutes (X-4)

What the text says. Every state has a breach notification law, and the requirements differ: whether a numeric deadline applies, what the notice must contain, which agencies receive it, and what remedies follow. We hold no state-by-state count of the applicant records outside New York and Pennsylvania. The next step is to obtain that count, then have counsel assess each applicable jurisdiction's current notice, timing, agency, and remedy requirements.

Citation and source status. statutes to be identified by counsel. No statute is summarized here. Counsel identifies the statutes after the state-by-state count is obtained.

Recorded times and the computed deadline. None. The bank has recorded no trigger and we compute nothing.

Facts relevant to it.

- Other states have 7,336 of the applicant records. We hold that count and no split by state.

Securities disclosure

SEC current report on a cybersecurity incident (CL-4)

What the text says. A registrant files an Item 1.05 Form 8-K for a cybersecurity incident it determines to be material, generally four business days after that determination. Instruction 1 to Item 1.05 says the materiality determination "must be made without unreasonable delay after discovery of the incident." Instruction 2 says that if the Item 1.05(a) information is not determined or is unavailable at filing, the registrant says so, and amends the report (Form 8-K/A) within four business days after the information is determined or becomes available. The filing can be postponed if the United States Attorney General determines, and tells the SEC in writing, that immediate disclosure would pose a substantial risk to national security or public safety. The SEC Corporation Finance Director's statement of May 21, 2024 is staff guidance, not a rule. It says that if a registrant chooses to disclose an incident before it has made a materiality determination, the staff encourages it to use a different item, such as Item 8.01. That creates no duty to make the voluntary disclosure; Item 1.05 applies after a materiality determination, subject to its requirements. The lengths of the delay periods in Item 1.05(c) are for counsel to read in the Form.

Citation and source status. Form 8-K, Item 1.05. Verified at a secondary copy of the primary text (Federal Register release 33-11216, 88 FR 51896). Counsel to confirm at the SEC's site.

Recorded times and the computed deadline. The bank recorded its materiality determination on Tuesday, July 14, 2026. The computed deadline is Monday, July 20, 2026, four business days later (July 15, 16, 17, and 20). The bank recorded the Form 8-K on Friday, July 17, 2026.

Facts relevant to it.

- The materiality determination is the registrant's and counsel's. We make no finding on it.
- The interval between the date entered as the discovery date (Saturday, July 4, 2026) and the recorded materiality determination (Tuesday, July 14, 2026) is 10 days. That is arithmetic only, and we do not assess it.
- The holding company is listed. The bank has $7.4 billion in assets and 61 branches.
- The fact in the Investigation's readout that was not available on July 9 is the count by state. The July 9 limits stand: the copy-out is probable, with high confidence, and not confirmed; object reads are unknown; no host access was found. Whether any bears on a later filing, or on an amendment under Instruction 2, is for counsel.

Suspicious activity reporting

Suspicious activity report (CL-5)

What the text says. 31 CFR 1020.320(b)(3) calls for a bank to file a suspicious activity report no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing. If no suspect is identified, the bank may delay filing for an additional 30 days to identify one, but in no case later than 60 days after initial detection. For violations that require immediate attention, the rule calls for immediate notification by telephone to an appropriate law-enforcement authority, in addition to filing. Section 1020.320(e)(1)(i) provides that no bank, "and no director, officer, employee, or agent of any bank" shall disclose a suspicious activity report or information that would reveal its existence. The confidentiality rule therefore reaches an agent of the bank, and whether Vantalect is one is for counsel.

Citation and source status. 31 CFR 1020.320(b)(3) and (e). Text of (b)(3) and (e) checked at the eCFR for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current text.

Where the clock is. This memo holds no suspicious activity report clock, review, filing, or non-filing status, and we will not record one in it. The clock is in the annex of the Notification-Clock Worksheets, which is paginated separately and delivered only to counsel and the BSA officer. Whether the confidentiality rule reaches Vantalect as an agent of the bank is for counsel.

Other federal and sector rules

FTC Safeguards Rule notice (CL-9)

What the text says. 16 CFR 314.4(j) calls for notice to the FTC "as soon as possible, and no later than 30 days after discovery of the event," where the notification event involves "at least 500 consumers." Discovery is "the first day on which such event is known to you." The notification applies to non-bank financial institutions under FTC jurisdiction. We list it only so that counsel can rule it out: the bank answers to the FDIC, and the FDIC's counterpart is 12 CFR 304.23 (CL-1), with the Interagency Guidance listed as X-6. Section 314.2 defines a notification event as acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Ruling it out is counsel's call.

Citation and source status. 16 CFR 314.4(j). Quoted from the rule's text. Counsel to confirm the current text.

Recorded times and the computed deadline. None. The bank has recorded no trigger and we compute nothing.

Facts relevant to it.

- The bank answers to the FDIC and NYDFS, and the holding company answers to the Federal Reserve. We list this rule only so counsel can rule it out.
- The count of applicant records is 412,317.

HIPAA breach notification (X-1)

What the text says. 45 CFR 164.404 calls for notice to individuals "without unreasonable delay" and no later than 60 calendar days after discovery of a breach. Discovery is the first day the breach is known, or would have been known with reasonable diligence. The knowledge of workforce members and agents is imputed to the covered entity. Law-enforcement delay is at 164.412. The notice to HHS and the media for breaches of 500 or more, and the business-associate duties at 164.410, were not verified.

Citation and source status. 45 CFR 164.404. Quoted from the rule's text. Counsel to confirm the current text.

Recorded times and the computed deadline. None. The bank has recorded no trigger and we compute nothing.

Facts relevant to it.

- The data types in the snapshot are names, Social Security numbers, dates of birth, and income. None of them is a health data type, but we have not reviewed the loan files.

CIRCIA covered-incident reporting (CL-10)

What the text says. CISA's web page states that organizations are not required to submit covered cyber incident or ransom payment reports under CIRCIA until the final rule takes effect, and that CISA continues to work on the final rule. The statute is codified at 6 U.S.C. 681b. It calls for a covered entity to report a covered cyber incident not later than 72 hours after it reasonably believes the incident has occurred, and a ransom payment not later than 24 hours after the payment, once the final rule requires reports.

Citation and source status. 6 U.S.C. 681b. Statute (6 U.S.C. 681b) and CISA's CIRCIA page checked for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm the current status of the final rule.

Recorded times and the computed deadline. None. The final rule is not in force, and we compute nothing.

Facts relevant to it.

- The bank reported to the FBI through IC3. Counsel decides whether to report to CISA as well.

Ransom and sanctions

The attacker demanded $14,500,000 in cryptocurrency by Tuesday, July 7, at 18:00 EDT. No payment was made, and we did not negotiate. The imported key material on the three attacker keys expired at that hour, and nothing the bank needs was under them.

OFAC. OFAC's updated advisory of September 21, 2021 says that companies that facilitate ransomware payments, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, "may risk violating OFAC regulations," and that the U.S. government "strongly discourages" paying ransom or extortion demands. OFAC may impose civil penalties on a strict liability basis, so a person may be liable without knowing a transaction was prohibited. License applications involving ransomware payments are reviewed case by case with a presumption of denial. OFAC says a prompt, complete report to law enforcement and full cooperation are significant mitigating factors, and it makes the outcome depend on the facts. That is not immunity. No payment was made in this incident, and counsel decides whether any of this bears on the bank.

The indicators for screening. The table gives counsel the indicators we hold, for counsel only. They are indicators and nothing more. They do not identify a person, and we make no sanctions determination. Whether and by whom they are screened is for counsel. Nothing in this table belongs in the Indicators of Compromise report unless counsel clears it.

Indicators for sanctions screening, for counsel only. The IDs in the note rows are the custody IDs in the Chain of Custody Log.

Indicator	Value	Source
Payment address in the ransom note	Withheld in this sample. The facts hold no payment address. In a real engagement we would give counsel every address exactly as printed in the sealed note copy, so counsel can check each against the digital currency addresses on the sanctions lists.	The sealed note copies below
Contact identifiers in the ransom note	Withheld in this sample, as the contact is. In a real engagement we would give counsel each identifier exactly as printed.	The sealed note copies below
Ransom note copy `EVD-002`	SHA-256 of the sealed copy `de415b24095cdbb614b6a7b8652762069bd72cc88022d8e44a7f8e8266f2265d`	Ransom note in the imaging archive bucket, with object metadata; sealed 04:09 EDT on Saturday, July 4
Ransom note copy `EVD-003`	SHA-256 of the sealed copy `1cb44b7976a154e6b82d0bf942b10efdbbf8b2195b859112d8e831dec88ada47`	Ransom note in the data lake bucket, with object metadata; sealed 04:12 EDT on Saturday, July 4
Ransom note copy `EVD-004`	SHA-256 of the sealed copy `6bab9ef7668b31adad451193ab1a14e2ff304d08fb332f39f22728871743a0d8`	Ransom note in the lending documents bucket, with object metadata; sealed 04:15 EDT on Saturday, July 4
Attacker AWS account	`777788889999`	Organization trail
Attacker address	`198.51.100.23`	Organization trail
Attacker address	`198.51.100.41`	Organization trail
Attacker address	`203.0.113.47`	Organization trail

The attribution cue. Our wording is "consistent with a Russian-speaking, financially motivated actor," under our tracking label `VTL-C1`, and our confidence is low. The basis is three cues. The discovery calls fell between 02:00 and 11:00 EDT on each of four days, a window that fits many time zones, Moscow among them, and working hours are easy to copy. The ransom note's object metadata carries Russian-language artifacts by our reading, with no linguistic analysis, and metadata can be planted. Our tooling and infrastructure notes overlap a cluster we track as `VTL-C1`, a label that is ours and names no real group. We name no group, country, or person, and none of this supports a sanctions determination.

FinCEN. FinCEN's ransomware advisory of November 8, 2021 (FIN-2021-A004) says that suspicious transactions involving ransomware attacks are "situations involving violations that require immediate attention," that a financial institution wanting to report one should contact the FinCEN Financial Institution Hotline, and that it must then file a suspicious activity report. No transaction with the attacker is recorded here, but the absence of a ransom payment does not itself resolve any suspicious activity report question. FinCEN's cyber-event advisory (FIN-2016-A005, October 25, 2016) says that a cyber-event that a bank knows, suspects, or has reason to suspect was intended, in whole or in part, to conduct, facilitate, or affect a transaction is part of an attempt to conduct a suspicious transaction, and that the funds and assets involved in or put at risk by the cyber-event are counted in aggregate against the $5,000 threshold. The BSA officer and counsel assess the threshold and the facts separately. The suspicious activity report clock, and any filing or non-filing status, stay in the worksheets' restricted annex and not in this memo.

What we will and will not do. We supply technical indicators. We do not recommend, negotiate, or carry out a payment, and we do not hold or move funds.

Preservation and litigation hold

We preserved the evidence we collected, and the bank's own hold is not a fact we have. The duty to preserve is for counsel. This section lists what we know, and it keeps the evidence apart from the recovery copies.

What was preserved

- An evidence account, `wf-ir-forensics`, was created at 03:12 EDT on July 4 in a new Incident OU, and evidence preservation began there. The Chain of Custody Log records each evidence item, and the final log comes at the close.
- Before the bank changed the share, the key policies, or the grant on July 4, we captured their state with the incident role: the snapshot's sharing attributes at 02:03 EDT, the three key policies from 02:03 to 02:04, and the grants from 02:04 to 02:05. The bank then removed the share and changed the policies as in the dates above.

- The organization trail kept recording through the incident. The attacker's attempt to stop it at 22:15 EDT on July 3 was denied.
- The attacker's user, its access key, and two roles were deleted on Wednesday, July 8, after preservation. The three attacker KMS keys were kept as they are for counsel. Their imported key material expired at 18:00 EDT on July 7, and `PendingImport` is the state they have been in since. The trail shows three `PutKeyPolicy` calls at 02:09 EDT on July 4 that dropped the outside account's statement from each key policy, and it shows the bank's three `DisableKey` calls on July 8, from 10:03:30 to 10:04:20 EDT, each rejected with `KMSInvalidStateException` because a key in that state cannot be disabled. The keys were not disabled, and no change to them succeeded on July 8.
- The imaging archive's current versions went through an S3 Batch Replication job into an Object Lock bucket in the vault. The replication rule set at 17:05 EDT on July 8 copies only objects written after it was set; the bank built a manifest of the current versions under its own key and started the job over them. The job ran from Wednesday, July 8, 18:25 EDT to Sunday, July 12, 21:40 EDT, 4 days 3 hours 15 minutes. It had 286,000,000 current versions in its manifest, 1,206 tasks failed (`SrcVersionNotFound`, the version was gone from the source), and the 122,600,000 noncurrent versions were not in the manifest, so the job did not copy them.

Recovery copies, not preserved evidence

These copies exist so the bank can recover. They are not in the custody register, and we do not list them as preserved evidence. Counsel decides whether any of them should be entered in the register with a retention counsel sets.

- **The 46 EBS snapshot copies.** They were shared with the vault account on Sunday, July 5, copied, and locked with `LockSnapshot` in compliance mode for 14 days, with a 72-hour cool-off, from 05:45 EDT on Monday, July 6. A 14-day lock set at that time ran out about July 20. The trail shows no event that extended or removed the lock after it was set, so as of July 24 the lock has lapsed. The vault OU's service control policy still denies `ec2:DeleteSnapshot` to every principal in the vault account.
- **The ten RDS snapshot copies.** They are plain snapshots and are not under any lock. They are protected by the vault OU's service control policy, which denies deletion and key changes to everyone, and by keys the bank holds. The weakest link is someone with Organizations rights in the management account who could change that policy.
- **The AWS Backup vault.** Vault Lock on `wf-recovery` covers one recovery point, of the database `wf-los-vault` that the bank restored in the vault account on July 6. Only the 46 EBS copies are both copied and under a lock.

What was not logged or was lost

- The attacker deleted the configuration of a legacy account trail at 22:14 EDT on July 3. Files it had already delivered remain unless separately deleted, and no such deletion is shown. We rely on the organization trail for that period.
- S3 data events recorded writes only, and the lending documents bucket has no data events. Object reads in the imaging archive and in that bucket are unknown.
- Containment and eradication changed live settings. The Containment and Eradication Actions report records who approved each step and what was captured before it.

What counsel may want to consider

- **The duty.** Federal Rule of Civil Procedure 37(e) applies when electronically stored information "should have been preserved in the anticipation or conduct of litigation" and a party "failed to take reasonable steps." Prejudice allows curative measures. Only "intent to deprive" allows an adverse-inference instruction, dismissal, or default. We quote the rule's text as published by the Legal Information Institute, and counsel should confirm it against the current text. When the duty arose is for counsel.
- **The hold.** Whether and when to issue a litigation hold, to whom, and whether it reaches the evidence account and our working copies is counsel's decision.
- **Chain of custody.** We record who collected each item, when, from which resource, how it was hashed, and every transfer. Rule 902(13) allows a record generated by an electronic process or system to be self-authenticating with a qualified person's certification, and Rule 902(14) does the same for data copied from an electronic device, storage medium, or file when it is authenticated by a process of digital identification. Whether and how the bank's counsel would use them is for counsel. NIST SP 800-86 is the federal reference on forensic technique in incident response, and it describes itself as an IT view and not legal advice.
- **Disposition.** We will ask counsel for instructions on our working copies and on the attacker KMS keys before the engagement closes.

Privilege and distribution

Whether privilege or work-product protection applies is counsel's analysis, and this memo does not offer one. These are the facts of our engagement that counsel may want in front of it.

- Counsel's three-party letter and the incident statement of work were signed at 00:52 EDT on Saturday, July 4. Counsel retained Vantalect under that letter, and the statement of work is specific to this incident.

- This memo goes to counsel only. Counsel decides whether the sponsor or anyone else receives it or the July 24 readout, and counsel keeps the distribution record.

Contracts that may carry notice duties

We have seen none of the bank's contracts, and the table lists the categories counsel may want to check, with the facts we can supply for each.

Contracts that may carry notice duties. We have read none of them.

Category	Why it may matter	Facts we can supply
Cyber insurance policy	Many policies call for prompt notice of a claim or circumstance, and for the insurer's consent to a vendor that is not on its panel.	The bank notified the broker's claims hotline at 01:15 EDT on July 4. The insurer's written consent arrived at 02:10 EDT. We have not seen the policy.
Managed security service provider agreement	The agreement may set response times and notice terms in both directions.	The provider received the GuardDuty finding at 22:44 EDT on July 3 and paged the on-call engineer at 23:18 EDT. We have not seen the agreement.
AWS customer agreement and acceptable-use terms	They may govern notice of security events and the access we were given.	Counsel's three-party letter and the incident statement of work, signed at 00:52 EDT on July 4, gave us written access. We have not read the AWS terms.
The contractor whose personal laptop held the stolen key	The contractor's agreement may carry security, notice, or indemnity terms.	Counsel's interview, not AWS evidence, is the source. It is outside our evidence.
Software and platform vendors	Vendors for the build system and the loan platform may have notice terms, or may hold data of their own.	The attacker's path used the bank's build role. The loan platform's logs show no attacker traffic. We have not seen the vendor contracts.
Customers, investors, and loan counterparties	Agreements about loan files held in the imaging archive may carry notice duties to the other party.	We have not seen them. The archive holds loan documents, and no object read is known, but reads were not logged.
Vantalect's own engagement	We hold copies of logs and evidence in the evidence account, and the engagement terms govern how.	Counsel is the contracting party for the incident. Whether any data-processing or business-associate terms are needed for what we hold is counsel's decision.

As we read it, New York's statute calls for a business that maintains data it does not own to tell the owner immediately (see CL-6). Whether the bank maintains any data for another party is a question for counsel.

The questions only counsel can answer

These are decisions and facts we cannot supply. Each is the bank's or counsel's. The first list gives the questions for the regimes whose citations, text, or facts are new or changed in this edition. The questions for the other regimes, and the suspicious activity report questions, are in the Notification-Clock Worksheets under the same ID. The second list holds questions that cut across regimes.

Questions by regime

- **CL-2.** Whether the event is a notification incident under the definition at 225.301, and whether Subpart N applies to the holding company, Wrenfield Bancorp, Inc.
- **CL-2.** Whether the holding company recorded its own determination, and when. Until it is obtained, the bank's recorded time is an illustration and not the holding company's trigger.
- **CL-2.** When the holding company gave its notice, and what receipt it holds.
- **X-6.** Whether the event is an incident of unauthorized access to or use of sensitive customer information, and whether the applicants in the loan records are customers within the guidance.
- **X-6.** When the bank became aware of the incident, and so when any notice to the FDIC, and to the Federal Reserve for the holding company, would be due as soon as possible.
- **X-6.** Who owns the reasonable investigation into the likelihood of misuse, and when it is complete.
- **X-6.** Whether the bank can say which customers' records were reached, and if it cannot, whether the group-of-files provision calls for notice to every customer in the group.
- **X-6.** Whether an appropriate law enforcement agency has made a written request to delay customer notice.
- **CL-3.** Whether the bank is a covered entity, and whether the incident meets any prong of the definition of a cybersecurity incident, including the ransomware prong.
- **CL-3.** The time of the determination, and what updates to the superintendent are due as the facts change.
- **CL-3.** Whether the incident at the bank, at an affiliate, or at a third-party service provider is the one that counts.

- **CL-6.** Whether the statute applies to the data involved, and what counts as private information, access, and acquisition under its text.
- **CL-6.** The discovery date. Counsel sets it, and Vantalect does not set or test it.
- **CL-6.** Whether notice to affected New York residents must be made in the most expedient time possible and without unreasonable delay, and no later than 30 days after discovery, subject to the law-enforcement delay in the statute.
- **CL-6.** Whether subdivision 2(b) removes the second individual notice only when the affected persons have already received a qualifying notice under a listed regime, and whether a notice to a regulator alone, such as the July 5 notice to DFS, meets that condition. We do not assume that it does.
- **CL-6.** Which of the state-office notices under 8(a) and the consumer reporting agency notice under 8(b) are still required, how many New York residents are notified, and whether that number is above the 5,000 that calls for consumer reporting agency notice.
- **X-3.** Whether the Act, as amended by Act 33 of 2024, applies to the Pennsylvania residents among the records, what it counts as personal information, and what section 3 requires and by when.
- **X-3.** Whether notice to the Pennsylvania Attorney General is called for under (c.1) because notice goes to more than 500 Pennsylvania residents, and whether any exemption applies.
- **X-3.** Whether section 5.4 applies because the bank reasonably believes a name with a Social Security number was accessed, and how the credit report and 12-month credit monitoring would be offered.
- **X-3.** Which other Pennsylvania offices, if any, receive notice.
- **CL-4.** Whether and when the registrant determined the incident to be material. Vantalect makes no materiality finding.
- **CL-4.** Whether the materiality determination was made without unreasonable delay after discovery, as Instruction 1 asks. Vantalect shows the interval between the two recorded dates as arithmetic only and does not assess it.
- **CL-4.** Whether any Item 1.05(a) information was undetermined or unavailable at filing, and whether Instruction 2 calls for an 8-K/A and by when.
- **CL-4.** How business days are counted, and whether any delay under Item 1.05(c) applies.
- **CL-4.** Whether an Item 8.01 filing, an amendment, or a later standalone Item 1.05 filing is called for as facts change.

Questions across regimes

1. Which of the regimes in this memo and in the clock worksheets apply to the bank and the holding company.

2. Whether 10:00 EDT on July 4 is the time of the bank's determination for each regime whose text turns on a determination.
3. The discovery date for each text, given the dates in this memo. The earliest attacker activity is June 29, the GuardDuty finding is July 3, and the bank recorded July 4. Vantalect does not say which is the discovery date.
4. Whether each statute turns on access, acquisition, or both, and what the evidence in this memo supports.
5. Whether the attacker's job that re-encrypted 61,300,000 imaging objects in place, under attacker keys and the job role's credentials, is access to or acquisition of the data in them under any text. We state what the job did and decide nothing.
6. Whether encryption under a key the attacker created affects any text. The attacker's account held a grant on that key while the share was open.
7. Whether the data types in the loan records are personal information, customer information, or nonpublic personal information under each text, and whether applicants are consumers.
8. Whether the check images and signature cards in the imaging archive carry customer information (a name with an account number), and whether anything must be learned from the bank about which objects hold what.
9. Whether the counts by state, which come from a query the bank ran and which Vantalect does not attest to, are the counts counsel will rely on, or whether counsel wants a second query or an independent check.
10. Whether any fact in the Investigation's readout calls for an update to NYDFS or any other regulator, or for an amendment to the Form 8-K or a separate filing. The materiality determination stays with the bank and counsel.
11. Whether any law-enforcement agency has asked, or may ask, that a notice be delayed. We have no record of one.
12. Whether counsel wants the ransom note's payment address and contact identifiers, which this sample withholds, given to it from the sealed note copies for screening.
13. Whether a litigation hold has been issued, to whom, and whether it reaches the evidence we hold.
14. Whether the 46 EBS snapshot copies in the vault, whose 14-day compliance lock ran out about July 20, are to be entered in the custody register with a retention counsel sets, or kept as recovery copies only.
15. Whether the ten RDS snapshot copies in the vault, which no lock covers, need more protection, given that someone with Organizations rights in the management account could change the service control policy that guards them.

16. How long to keep the three attacker KMS keys and the evidence account, and what to do with our working copies at the close.
17. Whether privilege or work-product protection applies to any report, and who may receive each.
18. Whether a facts-only summary should be prepared for counsel to release to regulators, insurers, and auditors.
19. Whether our role is to stay a consultant to counsel, or could become a testifying expert.
20. Whether state investigator-licensing rules bear on the work we do, and in which states. Counsel to identify the states and the rules.
21. Which insurance, vendor, customer, and investor contracts carry notice duties, and when each runs.
22. What data-processing or business-associate terms, if any, the bank needs from us for the evidence we hold.

Notice

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.