

Vantalect

AWS INCIDENT RESPONSE · SAMPLE DELIVERABLE

Notification-Clock Worksheets (Interim)

DISTRIBUTION: COUNSEL ONLY

Day 6: Interim worksheets · prepared for Wrenfield Bancorp, Inc.

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

July 9, 2026 · AWS Incident Response: The Response (July 4 to 9, 2026)

SAMPLE DELIVERABLE

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

A worksheet for counsel. Not legal advice. Vantalect makes no determination that any regime applies.

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 this worksheet is **2**

The clocks at a glance **4**

The worksheets **7**

CL-1. FDIC computer-security incident notification (12 CFR 304.23) 7

CL-2. Federal Reserve notification (holding company) (12 CFR 225.300 to 225.303 (Subpart N)) 8

CL-3. NYDFS cybersecurity incident notice (23 NYCRR 500.17(a)) 9

CL-4. SEC current report on a cybersecurity incident (Form 8-K, Item 1.05) 11

CL-6. New York GBL 899-aa (N.Y. Gen. Bus. Law 899-aa) 12

CL-7. NYDFS extortion payment notices (23 NYCRR 500.17(c)) 14

CL-8. OCC computer-security incident notification (12 CFR 53.3) 14

CL-9. FTC Safeguards Rule notice (16 CFR 314.4(j)) 15

CL-10. CIRCIA covered-incident reporting (6 U.S.C. 681b, background citation) 16

X-1. HIPAA breach notification (45 CFR 164.404) 17

X-2. Bank service provider rules (12 CFR 53.4 and 12 CFR 304.24) 17

X-3. Pennsylvania breach notification statute (Breach of Personal Information Notification Act, Act 94 of 2005, as amended by Act 33 of 2024) 18

X-4. Other state breach statutes (statutes to be identified by counsel) 19

X-5. OFAC sanctions considerations (OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021)) 20

X-6. Interagency Guidance on customer information incidents (GLBA Section 501(b)) 21

Counsel notes to the situation reports **23**

What would change this worksheet **24**

Annex S: SAR timing (counsel and the BSA officer only) **25**

Notice **27**

What this worksheet is

This is an interim worksheet, dated Thursday, July 9, 2026, and it shows only what the bank had recorded by that day. For each regime counsel may want to consider, it gives the decision owner, the trigger as the bank recorded it, the deadline we computed from that trigger, the status, the facts we can supply, and the questions only counsel can answer. We are Vantalect. We compute

from the times the bank entered. We do not decide whether any regime applies, whether anything is material, what the discovery date is, or whether any notice is due. Those decisions belong to the bank and to counsel, and this worksheet is not legal advice.

Who reads this, and what the label does

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.

Limits. Five things are not known on July 9, and the worksheet says so where they matter.

- Whether the registrant has determined the incident to be material. No determination is recorded.
- The split of the applicant records by state of residence. The count we carry is the working total.
- Whether the shared database snapshot was in fact copied out. We rate the copy-out probable, with high confidence. It is not confirmed.
- Whether any object in the imaging archive was read. Reads were not logged.
- Whether any other state, federal, or contract notice duty applies. That is for counsel.

What the status and difference columns mean. "Recorded" means the bank gave us a time for the notice or filing. "Not recorded" means the bank had given us no time on July 9. The difference column is the time between the recorded time and the computed time. It is arithmetic only. It is not a finding about any duty, and it is not a statement that any notice was timely. For an open clock it is the time from July 9 to the computed time. Counsel decides how each rule counts days and hours, and whether a weekend or holiday changes the count.

Where the texts come from. Each worksheet block says whether its text is quoted from the rule, quoted from text as we have it, taken from a secondary source, taken from an agency web page, or not retrieved. Counsel should check every quotation against the current official text. Source statuses that cite October 2026 record when this sample's research read the text. They are not something the bank or Vantalect knew in July.

The clocks at a glance

Of the five clocks this table tracks, four are computed on July 9 because each has a recorded trigger, three of those have a recorded notice, and the SEC clock has no trigger yet and is not computed. The bank's determination at 10:00 EDT on Saturday, July 4 is the trigger we use for the three notices to regulators. The discovery date counsel set is the trigger we use for the New York consumer-notice clock. The SEC clock waits for a materiality determination that has not been recorded. The table shows, for each recorded time, the arithmetic difference from the computed time, and nothing more. We do not say whether any notice was timely, because that depends on the trigger counsel and the bank take. CL-8 and CL-9 are listed only so that counsel can rule them out, for the reasons in their blocks.

One clock is kept in Annex S for counsel and the BSA officer only.

The regimes this worksheet lists, except the one in Annex S. Deadlines are computed from the times the bank entered. Whether a regime applies is for the bank and counsel.

ID	Regime	Decision owner	Trigger as recorded	Computed deadline	Status on July 9	Difference between recorded time and computed time (arithmetic only)
CL-1	FDIC computer-security incident notification (12 CFR 304.23)	Bank (the determination)	Bank's determination, Saturday, July 4, 10:00 EDT	Sunday, July 5, 22:00 EDT	Notice recorded July 4, 14:30 EDT	1 day 7 hours 30 minutes earlier than the computed time
CL-2	Federal Reserve notification (holding company) (12 CFR 225.300 to 225.303 (Subpart N))	Bank (the determination)	Unverified for the holding company. The bank's recorded determination, Saturday, July 4, 10:00 EDT, is its own	Unverified for the holding company. Illustration if it also determined at the bank's recorded time: Sunday, July 5, 22:00 EDT	Notice recorded July 4, 14:45 EDT	1 day 7 hours 15 minutes earlier than the illustrative time, if the holding company's determination matched the bank's
CL-3	NYDFS cybersecurity incident notice (23 NYCRR 500.17(a))	Bank (the determination)	Bank's determination, Saturday, July 4, 10:00 EDT	Tuesday, July 7, 10:00 EDT	Notice recorded July 5, 11:15 EDT	1 day 22 hours 45 minutes earlier than the computed time
CL-4	SEC current report on a cybersecurity incident (Form 8-K, Item 1.05)	Bank and counsel (the materiality determination)	None recorded	Not computed	No trigger recorded	Not computed
CL-6	New York GBL 899-aa (N.Y. Gen. Bus. Law 899-aa)	Counsel (the discovery date)	Discovery date counsel set, July 4	Monday, August 3, 2026	Not recorded on July 9	No recorded time. 25 calendar days from July 9 to the computed time
CL-7	NYDFS extortion payment notices (23 NYCRR 500.17(c))	Bank	None recorded	Not computed	Not triggered. No payment is recorded	Not computed
CL-8	OCC computer-security incident notification (12 CFR 53.3)	Counsel	None recorded	Not computed	Listed only so counsel can rule it out	Not computed
CL-9	FTC Safeguards Rule notice (16 CFR 314.4(j))	Counsel	None recorded	Not computed	Listed only so counsel can rule it out	Not computed

ID	Regime	Decision owner	Trigger as recorded	Computed deadline	Status on July 9	Difference between recorded time and computed time (arithmetic only)
CL-10	CIRCIA covered-incident reporting (6 U.S.C. 681b, background citation)	Counsel	None recorded	Not computed	Final rule not in force; counsel to confirm on the day	Not computed

Other regimes counsel may want to consider. We list them so that nothing is left off the page. None has a trigger the bank has recorded, and we compute nothing for them.

ID	Regime	Decision owner	Trigger as recorded	Computed deadline	Status on July 9
X-1	HIPAA breach notification (45 CFR 164.404)	Counsel	None recorded	Not computed	Counsel decides whether the regime applies
X-2	Bank service provider rules (12 CFR 53.4 and 12 CFR 304.24)	Counsel	None recorded	Not computed	Counsel decides whether the regime applies
X-3	Pennsylvania breach notification statute (Breach of Personal Information Notification Act, Act 94 of 2005, as amended by Act 33 of 2024)	Counsel	None recorded	Not computed	Counsel decides. Not computed
X-4	Other state breach statutes (statutes to be identified by counsel)	Counsel	None recorded	Not computed	Counsel decides. Not computed
X-5	OFAC sanctions considerations (OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021))	Counsel	None recorded	Not computed	No clock. Considerations for counsel
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)	Counsel	None recorded	Not computed	No clock. Guidance with no deadline in days

The worksheets

Each block below repeats the glance row in full, then gives the rule's text, the source status of that text, the facts we can supply on July 9, and counsel's questions. The first five blocks, CL-1 to CL-4 and CL-6, are the five clocks this worksheet tracks, and CL-4 is not computed on July 9. CL-7 to CL-10 and X-1 to X-6 are regimes with no trigger the bank has recorded. CL-8 and CL-9 are listed only so that counsel can rule them out. X-6 is guidance with no deadline in days, so we compute nothing for it.

CL-1. FDIC computer-security incident notification (12 CFR 304.23)

- **Decision owner:** Bank (the determination).
- **Trigger as the bank recorded it:** Bank's determination, Saturday, July 4, 10:00 EDT.
- **Computation:** 36 hours after Saturday, July 4, 10:00 EDT is Sunday, July 5, 22:00 EDT (02:00 UTC on Monday, July 6, 2026).
- **Computed deadline:** Sunday, July 5, 22:00 EDT.
- **Status on July 9:** Notice recorded July 4, 14:30 EDT. Arithmetic only: 1 day 7 hours 30 minutes earlier than the computed time.

What the rule's 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.

Source status. Quoted from the rule's text. Counsel to confirm the current text.

Facts we can supply on July 9.

- The bank held its determination meeting at 10:00 EDT on Saturday, July 4, with Harold Penwick, Mireille Danvers, Anand Sethuraman, and outside counsel. 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.
- The bank recorded the notice to the FDIC at 14:30 EDT and the notice to the Federal Reserve at 14:45 EDT, both on Saturday, July 4.

- Loan origination was offline from 01:50 EDT on July 4 to 16:00 EDT on Wednesday, July 8: 110 hours 10 minutes. The bank took it offline itself to freeze its state, and 1,912 applications queued.
- In the imaging archive, 61,300,000 of 286,000,000 objects (21.4%) were re-encrypted under keys the attacker created. The bank rewrote them under its own key and reports that its check at 14:00 EDT on July 7 found 0 current objects under any attacker key (bank-reported; the query results are not independently preserved).
- We make no finding on whether these facts meet the rule's definition of a notification incident.

Questions only counsel can answer.

- Whether the regime applies to the bank, and whether the event meets the rule's definition of a notification incident.
- The time at which the bank determined that a notification incident had occurred, and whether the time the bank recorded is that time.
- Whether the 36 hours are counted as clock hours across the weekend, and what the notice needed to contain.

CL-2. Federal Reserve notification (holding company) (12 CFR 225.300 to 225.303 (Subpart N))

- **Decision owner:** Bank (the determination).
- **Trigger as the bank recorded it:** Unverified for the holding company. The bank's recorded determination, Saturday, July 4, 10:00 EDT, is its own.
- **Computation:** Illustration if the holding company also determined at Saturday, July 4, 10:00 EDT: 36 hours after that time is Sunday, July 5, 22:00 EDT (02:00 UTC on Monday, July 6, 2026). The period runs from each banking organization's own determination, so this is not a computed limit.
- **Computed deadline:** Unverified for the holding company. Illustration if it also determined at the bank's recorded time: Sunday, July 5, 22:00 EDT.
- **Status on July 9:** Notice recorded July 4, 14:45 EDT. Arithmetic only: 1 day 7 hours 15 minutes earlier than the illustrative time, if the holding company's determination matched the bank's.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The holding company is Wrenfield Bancorp, Inc. The bank is Wrenfield Bank, a New York-chartered commercial bank, not a Federal Reserve member.
- The bank's recorded determination and notices are the same as in CL-1. The Federal Reserve notice is recorded at 14:45 EDT on Saturday, July 4.
- We do not know whether the holding company recorded a separate determination. The 36 hours run from each banking organization's own determination, so the bank's time is not the holding company's trigger unless the holding company made the same determination. Obtain the holding company's recorded determination and its notification receipt before treating any deadline as the actual limit.

Questions only counsel can answer.

- 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.
- 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.
- When the holding company gave its notice, and what receipt it holds.

CL-3. NYDFS cybersecurity incident notice (23 NYCRR 500.17(a))

- **Decision owner:** Bank (the determination).
- **Trigger as the bank recorded it:** Bank's determination, Saturday, July 4, 10:00 EDT.
- **Computation:** 72 hours after Saturday, July 4, 10:00 EDT is Tuesday, July 7, 10:00 EDT (14:00 UTC on Tuesday, July 7, 2026).
- **Computed deadline:** Tuesday, July 7, 10:00 EDT.
- **Status on July 9:** Notice recorded July 5, 11:15 EDT. Arithmetic only: 1 day 22 hours 45 minutes earlier than the computed time.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The bank recorded the NYDFS notice at 11:15 EDT on Sunday, July 5.
- The first write-capable attacker session in production began at 21:04 EDT on Friday, July 3. The first use of the stolen key we have found is Monday, June 29, 03:14 EDT.
- Everything found so far happened inside the bank's own AWS accounts, through credentials issued to the bank's service user. We have not found a service provider's system in the chain.
- No payment was made, so the extortion-payment notices in CL-7 have no trigger.
- The amended definition of a cybersecurity incident reaches an event at the covered entity, its affiliates, or a third-party service provider, and one prong is the deployment of ransomware within a material part of the information systems. We do not apply any prong. The facts that bear on them are that the attacker re-encrypted 61,300,000 of 286,000,000 imaging archive objects under keys it created, that loan origination was offline, and that the activity was in the bank's own accounts, with no service provider's system found in the chain.
- We have not seen the notice the bank sent, so we cannot say what it contained or whether updates have followed.

Questions only counsel can answer.

- 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.

- The time of the determination, and what updates to the superintendent are due as the facts change.
- Whether the incident at the bank, at an affiliate, or at a third-party service provider is the one that counts.

CL-4. SEC current report on a cybersecurity incident (Form 8-K, Item 1.05)

- **Decision owner:** Bank and counsel (the materiality determination).
- **Trigger as the bank recorded it:** None recorded.
- **Computation:** Not computed. No trigger is recorded, so there is nothing to count from.
- **Computed deadline:** Not computed.
- **Status on July 9:** No trigger recorded.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The holding company is listed. The bank has $7.4 billion in assets, 61 branches, and 1,240 employees.
- The attacker held write-capable access for 4 hours 18 minutes before the containment policy was attached at 01:22 EDT on Saturday, July 4. The earlier read-only activity began 4 days, 17 hours, 50 minutes before the first write.
- Loan origination was offline for 110 hours 10 minutes, and 1,912 applications queued. It returned after integrity checks.

- The shared database snapshot holds 412,317 applicant records (our working figure). The data types are names, Social Security numbers, dates of birth, and income.
- Containment was declared in writing by Mireille Danvers at 09:00 EDT on Thursday, July 9.
- No payment was made. The demand was $14,500,000 in cryptocurrency by Tuesday, July 7, at 18:00 EDT.
- The bank has recorded no materiality determination on July 9, so there is no interval from discovery to a determination to show. The discovery date counsel set is Saturday, July 4, 2026, and 5 calendar days have passed to July 9. That is arithmetic only. Instruction 1 to Item 1.05 asks that the determination be made without unreasonable delay after discovery, and we do not assess it. Counsel decides which date counts as discovery.
- Instruction 2 asks for a Form 8-K/A within four business days after information that was undetermined or unavailable at filing is determined or becomes available. No filing is recorded on July 9, so there is nothing to compare.
- We make no finding on materiality and will add facts when counsel asks.

Questions only counsel can answer.

- Whether and when the registrant determined the incident to be material. Vantalect makes no materiality finding.
- 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.
- 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.
- How business days are counted, and whether any delay under Item 1.05(c) applies.
- Whether an Item 8.01 filing, an amendment, or a later standalone Item 1.05 filing is called for as facts change.

CL-6. New York GBL 899-aa (N.Y. Gen. Bus. Law 899-aa)

- **Decision owner:** Counsel (the discovery date).
- **Trigger as the bank recorded it:** Discovery date counsel set, July 4.
- **Computation:** 30 calendar days after Saturday, July 4, 2026 is Monday, August 3, 2026.
- **Computed deadline:** Monday, August 3, 2026.
- **Status on July 9:** Not recorded on July 9. Arithmetic only: No recorded time. 25 calendar days from July 9 to the computed time.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- Counsel set Saturday, July 4, 2026 as the discovery date. We use it as given.
- Earlier dates are in the logs. The earliest attacker activity we have found is Monday, June 29, 03:14 EDT (read-only calls from `198.51.100.23`), and the GuardDuty finding is at 22:44 EDT on July 3. Whether either bears on discovery is for counsel.
- A copy of the loan origination database was shared with account `777788889999` at 23:51 EDT on July 3. Between 00:06 and 00:51 EDT on July 4, principals in that account made 7 calls on the key that protected the copy, logged in the bank's account. That is the pattern of a snapshot copy. We rate the copy-out probable, with high confidence. We did not see the data leave, and we do not call it confirmed.
- The snapshot holds 412,317 applicant records (working figure): names, Social Security numbers, dates of birth, and income. We do not yet have the split by state of residence.
- The statute's consumer reporting agency notice turns on more than 5,000 New York residents being notified. We do not yet have the New York count, and the number notified is for the bank and counsel.
- Whether notice under the Gramm-Leach-Bliley Act or Part 500 removes the second individual notice, and which state offices are still notified, is for counsel.
- Whether the data counts as private information under the statute, and whether it was accessed or acquired, are for counsel.

Questions only counsel can answer.

- Whether the statute applies to the data involved, and what counts as private information, access, and acquisition under its text.
- The discovery date. Counsel sets it, and Vantalect does not set or test it.
- 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.

- 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.
- 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.

CL-7. NYDFS extortion payment notices (23 NYCRR 500.17(c))

- **Decision owner:** Bank.
- **Trigger as the bank recorded it:** None. No payment is recorded.
- **Computation:** Not computed. The rule counts from a payment.
- **Computed deadline:** None.
- **Status on July 9:** Not triggered. No payment is recorded.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The bank recorded no payment to the attacker as of July 9.
- The attacker's deadline, Tuesday, July 7, at 18:00 EDT, has passed. The imported key material on the three attacker keys expired then, and nothing the bank needs was under them.

Questions only counsel can answer.

- Whether any later event, such as a payment by anyone on the bank's behalf, would start these periods.

CL-8. OCC computer-security incident notification (12 CFR 53.3)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None. The bank is state-chartered.

- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Listed only so counsel can rule it out.

What the rule's 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.

Source status. Quoted from the rule's text. Counsel to confirm the current text.

Facts we can supply on July 9.

- The bank is a New York-chartered commercial bank and not a Federal Reserve member. Its federal regulator is the FDIC.
- The bank has 61 branches. We have not seen any OCC-supervised affiliate in the facts.

Questions only counsel can answer.

- Whether the OCC's rule has any bearing on this bank or on an affiliate. Counsel can rule it out.

CL-9. FTC Safeguards Rule notice (16 CFR 314.4(j))

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None. The bank is supervised by bank regulators.
- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Listed only so counsel can rule it out.

What the rule's 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.

Source status. Quoted from the rule's text. Counsel to confirm the current text.

Facts we can supply on July 9.

- The bank answers to the FDIC and NYDFS, and the holding company answers to the Federal Reserve.
- The rule counts consumers affected, with a threshold of 500. The working count of applicant records is 412,317. Whether applicants are "consumers" under the rule is for counsel.

Questions only counsel can answer.

- Whether the rule reaches the bank or any affiliate, given that the bank answers to bank regulators. Counsel can rule it out.
- If it did, the date on which the event was first known.

CL-10. CIRCIA covered-incident reporting (6 U.S.C. 681b, background citation)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None. The final rule is not in force.
- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Final rule not in force; counsel to confirm on the day.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- If the final rule were in force, a ransom payment report would have no trigger here, because no payment was made.
- The bank has reported to the FBI through IC3. Our understanding is that a victim needs to report only once for the other agencies to be told, and counsel should confirm it. Counsel decides whether to report to CISA as well.

Questions only counsel can answer.

- Whether the final rule is in force on the day counsel reads this, and whether the bank would be a covered entity.
- Whether to report voluntarily to CISA or the FBI. CISA encourages voluntary sharing of cyber incident information before the final rule takes effect.

X-1. HIPAA breach notification (45 CFR 164.404)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None recorded.
- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Counsel decides whether the regime applies.

What the rule's 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.

Source status. Quoted from the rule's text. Counsel to confirm the current text.

Facts we can supply on July 9.

- The data types recorded for 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 contents of the loan files and counsel should ask the bank.
- 412,317 applicant records is the working count.

Questions only counsel can answer.

- Whether the bank, or any part of it, is a covered entity or business associate, and whether any record in the snapshot is protected health information.

X-2. Bank service provider rules (12 CFR 53.4 and 12 CFR 304.24)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None recorded.
- **Computation:** Not computed.
- **Computed deadline:** None.

- **Status on July 9:** Counsel decides whether the regime applies.

What the rule's 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.

Source status. Quoted from the rule's text. Counsel to confirm the current text.

Facts we can supply on July 9.

- The managed security service provider received the GuardDuty finding at 22:44 EDT and paged Owen Tribble at 23:18 EDT on July 3, 34 minutes later.
- We found no outage of an AWS service or of a provider's system. The disruption we found was to the bank's own workloads: loan origination for 110 hours 10 minutes, and the imaging archive objects the attacker re-encrypted.

Questions only counsel can answer.

- Whether any provider to the bank, including the managed security service provider, had a duty to notify the bank, and whether the bank is itself a provider to any other bank.
- Whether Vantalect, which delivers incident response and forensics under counsel's letter, is a bank service provider.

X-3. Pennsylvania breach notification statute (Breach of Personal Information Notification Act, Act 94 of 2005, as amended by Act 33 of 2024)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None recorded.
- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Counsel decides. Not computed.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The working count is 412,317 applicant records in total. We do not yet have the number who live in Pennsylvania. The Investigation will give counsel the split by state of residence.

Questions only counsel can answer.

- 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.
- 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.
- 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.
- Which other Pennsylvania offices, if any, receive notice.

X-4. Other state breach statutes (statutes to be identified by counsel)

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None recorded.
- **Computation:** Not computed.
- **Computed deadline:** None.
- **Status on July 9:** Counsel decides. Not computed.

What the rule's 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.

Source status. No statute is summarized here. Counsel identifies the statutes after the state-by-state count is obtained.

Facts we can supply on July 9.

- The only statute the bank has tied to a recorded date is New York's (CL-6). For every other state, the residents' counts are not yet available.
- Counsel may want the state-by-state split before choosing the statutes to read first.

Questions only counsel can answer.

- Which states' statutes apply to the residents of other states, and whether any state's numeric deadline runs from a different date than the discovery date counsel set.
- Whether notice goes to state attorneys general or other agencies, and when.

X-5. OFAC sanctions considerations (OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021))

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None. This is not a deadline.
- **Computation:** Not computed. No payment is recorded.
- **Computed deadline:** None.
- **Status on July 9:** No clock. Considerations for counsel.

What the rule's text says. OFAC's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (September 21, 2021) says that OFAC may impose civil penalties for sanctions violations on a strict liability basis, so a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know that it was engaging in a prohibited transaction. It says that companies that facilitate ransomware payments on behalf of victims, 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. License applications involving ransomware payments are reviewed case by case with a presumption of denial. OFAC says it will consider a self-initiated and complete report of an attack to law enforcement or other relevant

agencies, made as soon as possible after discovery, and full and ongoing cooperation, to be significant mitigating factors in an enforcement response. The outcome depends on the facts, and the advisory does not promise immunity. No payment was made in this incident.

Source status. Advisory text read in the Treasury PDF for the October 2026 publication of this sample, which the bank did not have in July. Counsel to confirm any later OFAC guidance.

Facts we can supply on July 9.

- The demand is $14,500,000 in cryptocurrency by Tuesday, July 7, at 18:00 EDT. The contact in the ransom note is withheld from this report.
- No payment was made, and we did not negotiate or contact the attacker.
- The indicators we can give counsel for screening are account `777788889999` and the addresses `198.51.100.23`, `198.51.100.41`, `203.0.113.47`. These are indicators. They are not an identification of a person or group, and we make no sanctions determination.

Questions only counsel can answer.

- Whether any screening of the attacker's indicators against sanctions lists is called for, and who performs it. Vantalect supplies indicators and makes no sanctions determination.
- Whether any future contact with the attacker, or any payment by anyone, is contemplated. Vantalect will not negotiate or carry out a payment.

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

- **Decision owner:** Counsel.
- **Trigger as the bank recorded it:** None. This is guidance with no deadline in days.
- **Computation:** Not computed. The guidance sets no deadline in days.
- **Computed deadline:** None.
- **Status on July 9:** No clock. Guidance with no deadline in days.

What the rule's 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.

Source status. 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.

Facts we can supply on July 9.

- The loan database snapshot holds 412,317 applicant records (our working figure): names, Social Security numbers, dates of birth, and income. We do not yet have the split by state of residence. These are counts of records, not of customers.
- The imaging archive (412 TB) holds loan files, check images, and signature cards (names with account numbers). We could not tell whether any object was read, because reads were not logged, so we do not say whose files were reached.
- The bank recorded its notice to the FDIC at 14:30 EDT on Saturday, July 4 and its notice to the Federal Reserve at 14:45 EDT on the same day. Those are the notices recorded under CL-1 and CL-2. Whether either is also the notice the guidance describes is for counsel.
- We have not seen any customer notice, and the bank has given us no law enforcement request to delay one.

Questions only counsel can answer.

- 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.
- 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.
- Who owns the reasonable investigation into the likelihood of misuse, and when it is complete.
- 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.

- Whether an appropriate law enforcement agency has made a written request to delay customer notice.

Counsel notes to the situation reports

The situation reports (Report 1) are operational and carry no legal content. The counsel items that were in them are gathered here for counsel alone. Each row is a neutral question or fact, taken as the bank's team raised it, with the place in this worksheet that answers it. No row records a decision, and none records a status for any filing.

Counsel items from the situation reports, one row per report that had one. Reports SR-10, SR-11, SR-14, and SR-15 had none.

Report	Date and time	Counsel item	Answered in
SR-01	Saturday, July 4, 01:00 EDT	The bank had made no determination. Which clock may run, and when, is counsel's decision.	CL-1
SR-02	Saturday, July 4, 02:00 EDT	The bank had made no determination.	CL-1
SR-03	Saturday, July 4, 03:00 EDT	The bank had made no determination.	CL-1
SR-04	Saturday, July 4, 04:00 EDT	The bank had made no determination.	CL-1
SR-05	Saturday, July 4, 05:00 EDT	The bank's determination meeting, with counsel, was set for 10:00 EDT. No determination yet.	CL-1
SR-06	Saturday, July 4, 09:30 EDT	No window that runs from the bank's determination had started, because no determination had been made. Counsel was to have the interim worksheets.	CL-1, CL-2, CL-3
SR-07	Saturday, July 4, 21:30 EDT	The bank's 10:00 EDT determination; the 36-hour and 72-hour windows computed from it; a timing question that is kept in Annex S; screening the attacker's indicators for sanctions.	CL-1, CL-2, CL-3, Annex S, X-5
SR-08	Sunday, July 5, 09:30 EDT	Time left on the NYDFS window; FDIC and Federal Reserve notices given the day before.	CL-1, CL-2, CL-3
SR-09	Sunday, July 5, 21:30 EDT	Whether the bank wants to tell customers anything (counsel's call); the regulator windows computed from the determination; the NYDFS notice given.	X-6, CL-1, CL-3

Report	Date and time	Counsel item	Answered in
SR-12	Tuesday, July 7, 09:30 EDT	The NYDFS computed window ended at 10:00 EDT that day; the notice had been given.	CL-3
SR-13	Tuesday, July 7, 21:30 EDT	A holding statement in case the attacker publishes: wording and timing are counsel's call.	Not in this worksheet. Counsel's call
SR-16	Thursday, July 9, 09:30 EDT	Whether and when the bank makes a materiality determination (none recorded); further notifications, if any; the windows that run from July 4 if counsel treats it as the date.	CL-4, X-1 to X-6, CL-6, Annex S

What would change this worksheet

Four events would add a trigger or a fact, and each is the bank's or counsel's to record. We will bring the worksheet up to date at the Investigation's readout.

- A materiality determination would give the SEC clock a trigger. We would then compute four business days from the date the bank enters.
- Counsel's decision on which state statutes apply would turn the other-state rows from "counsel decides" into computed clocks, if counsel gives us a trigger.
- A change in the discovery date, or in the date of initial detection, would move the New York deadline and the deadline in Annex S. We would recompute from the new date and show both.
- A payment by anyone would start the extortion-payment clock in CL-7.

What this worksheet does not cover. It does not cover contracts or insurance policies, which may carry their own notice duties and are for counsel. It does not cover the bank's own policies. It does not cover how a regulator will count time.

Annex S: SAR timing (counsel and the BSA officer only)

Page S-1 of S-2. This annex is separately paginated: its two pages are S-1 and S-2 in this text. It may be detached from the worksheet, and it goes only to counsel and the BSA officer, Colette Marsh. Vantalect records no review, filing, or non-filing status for any suspicious activity report, here or in any other document. The confidentiality rule below bars disclosing a report, or information that would reveal its existence, and whether it reaches Vantalect is for counsel.

What the rule's 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.

Source status. 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.

Page S-2 of S-2. Days from the date of initial detection (arithmetic only).

- **Date entered:** the bank entered Saturday, July 4, 2026 as the date of initial detection. Counsel and the BSA officer decide whether that is the date the rule counts from.
- **Computation:** 30 calendar days after Saturday, July 4, 2026 is Monday, August 3, 2026.
- **Time left:** 25 calendar days from July 9 to that date. This is arithmetic. It says nothing about any report.
- **Outer limit:** if the rule's extended period applied, 60 days counted from July 4 would run to Wednesday, September 2, 2026. Whether any extension is available is for the BSA officer and counsel.

Facts we hold that bear on the timing.

- The attacker account is `777788889999`. The addresses we have seen are `198.51.100.23`, `198.51.100.41`, `203.0.113.47`.
- The attacker demanded $14,500,000 in cryptocurrency. No payment was made, and we have not seen any funds move to the attacker.
- 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 identified no person. We have not computed a loss amount, and this annex does not assume one.

Questions only counsel can answer.

- Whether the confidentiality rule at 1020.320(e) reaches Vantalect as an agent of the bank, and who may receive the annex that holds this clock.
- The bank's date of initial detection, if the bank enters one. Vantalect computes days from a bank-entered date as arithmetic only, and records no review, filing, or non-filing status.
- Whether a cyber-event that did not end in a ransom payment or a completed transaction still triggers a report. FinCEN's advisory FIN-2016-A005 treats a cyber-event as part of an attempt to conduct a suspicious transaction when the bank knows, suspects, or has reason to suspect it was intended to conduct, facilitate, or affect a transaction, and the BSA officer and counsel assess the threshold and facts separately.
- Whether the 30-day period or the extended period would apply.
- Whether either law enforcement contact bears on the rule's call for immediate notice of violations that need it.

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.