

WELCOME TO

A Case Study of What NOT to Do in Vendor Management

Leticia Saiid, Security+
Chief of Staff & Chief Learning Officer
CoNetrix, LLC

DISCLAIMER

- **This presentation is for information only.**
Evaluate risks before acting on ideas from this session.
- **This presentation contains opinions of the presenters.**
Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
Unauthorized release of this information is prohibited.
Original material is copyright © 2023 Tandem.

SESSION INFO



AUDIO / VIDEO

If you cannot hear sound or see the presentation now, adjust or change your settings.



SURVEY

At the end, fill out the survey for a chance to win an Amazon gift card.



RESOURCES

The slides, a recording, and certificate of attendance will be sent via email.



QUESTIONS

Use the "Questions" panel to chat with the presenter and Tandem team.

ABOUT THE PRESENTER



Leticia Saiid

Security+

Chief of Staff & Chief Learning Officer

After earning a B.A. and a M.A. in Mathematics, Leticia joined CoNetrix, where she served as the Tandem Software Support Manager for several years. She built and directed Tandem's first team of support specialists. Leticia now serves as Chief of Staff & Chief Learning Officer where she focuses on corporate strategy, employee development, and training. In her free time, she enjoys mentoring college students, learning piano, and solving jigsaw puzzles.

[LinkedIn.com/in/LeticiaSaiid](https://www.linkedin.com/in/LeticiaSaiid)



About Me

TRAINING & ADVISING



-  Audit Management
-  Business Continuity Plan
-  Compliance Management
-  Cybersecurity
-  Identity Theft Prevention
-  Incident Management
-  Internet Banking Security
-  Phishing
-  Policies
-  Risk Assessment
-  Vendor Management



Tandem™

A CoNetrix company

Are you outsourcing any vendor management due diligence processes?

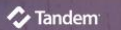
- Yes, determining what documents to get
- Yes, gathering documents
- Yes, reviewing documents
- No.

AGENDA

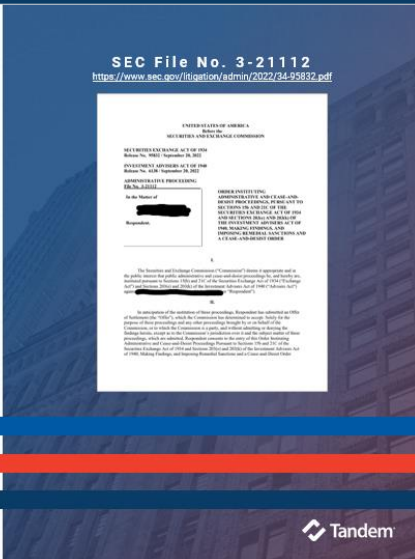
Subcontractors Guidance



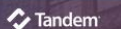
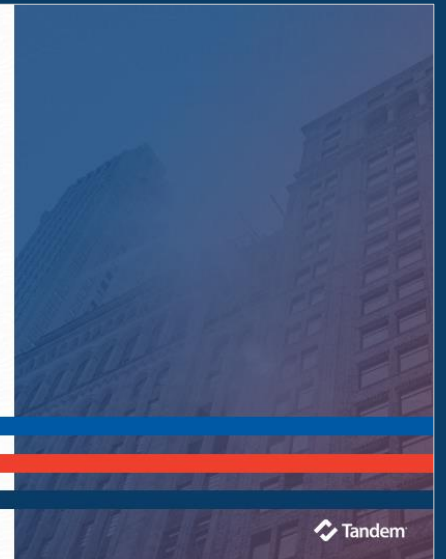
If-Then Due Diligence Method



A Cautionary Tale Case Study



Lessons Learned



Subcontractors Guidance



NEW THIRD-PARTY RISK MANAGEMENT GUIDANCE



FDIC FIL-44-2008

Guidance for Managing Third-Party Risk

June 6, 2008



OCC Bulletin 2013-29

Third-Party Relationships: Risk Management Guidance

October 30, 2013



FRB SR 13-19

Guidance on Managing Outsourcing Risk

December 5, 2013



OCC Bulletin 2017-21 | OCC Bulletin 2020-10

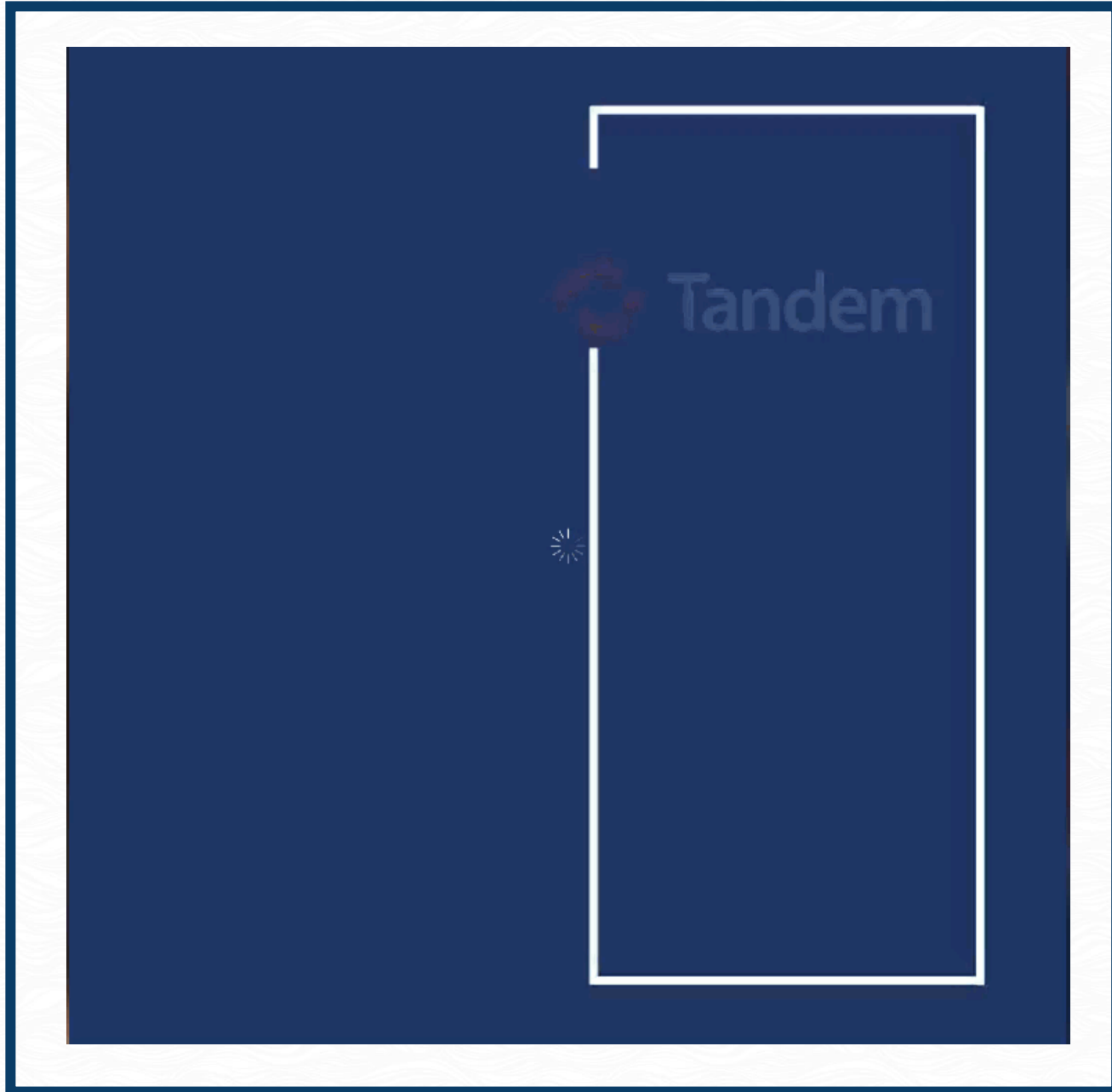
Third-Party Relationship: Frequently Asked Questions

June 7, 2017 | March 5, 2020

FEDERAL RESERVE SYSTEM
[Docket No. OP-1752]
FEDERAL DEPOSIT INSURANCE CORPORATION
RIN 3064-ZA26
DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency
[Docket ID OCC-2021-0011]
Interagency Guidance on Third-Party Relationships: Risk Management
AGENCY: The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), Treasury.
ACTION: Final interagency guidance.
SUMMARY: The Board, FDIC, and OCC (collectively, the agencies) are issuing final guidance on managing risks associated with third-party relationships. The final guidance offers the agencies' views on sound risk management principles for banking organizations when developing and implementing risk management practices for all stages in the life cycle of third-party relationships. The final guidance states that sound third-party risk management takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship. The agencies are issuing this joint guidance to promote consistency in supervisory approaches; it replaces each agency's existing general guidance on this topic and is directed to all banking organizations supervised by the agencies.
DATE: The guidance is final as of June 6, 2023.
FOR FURTHER INFORMATION CONTACT:
Board: Kavita Jain, Deputy Associate Director, (202) 452-2062, Chandni Saxena, Manager, (202) 452-2357, Timothy Geisbecker, Lead Financial Institution and Policy
1

Proposed: 07/19/2021

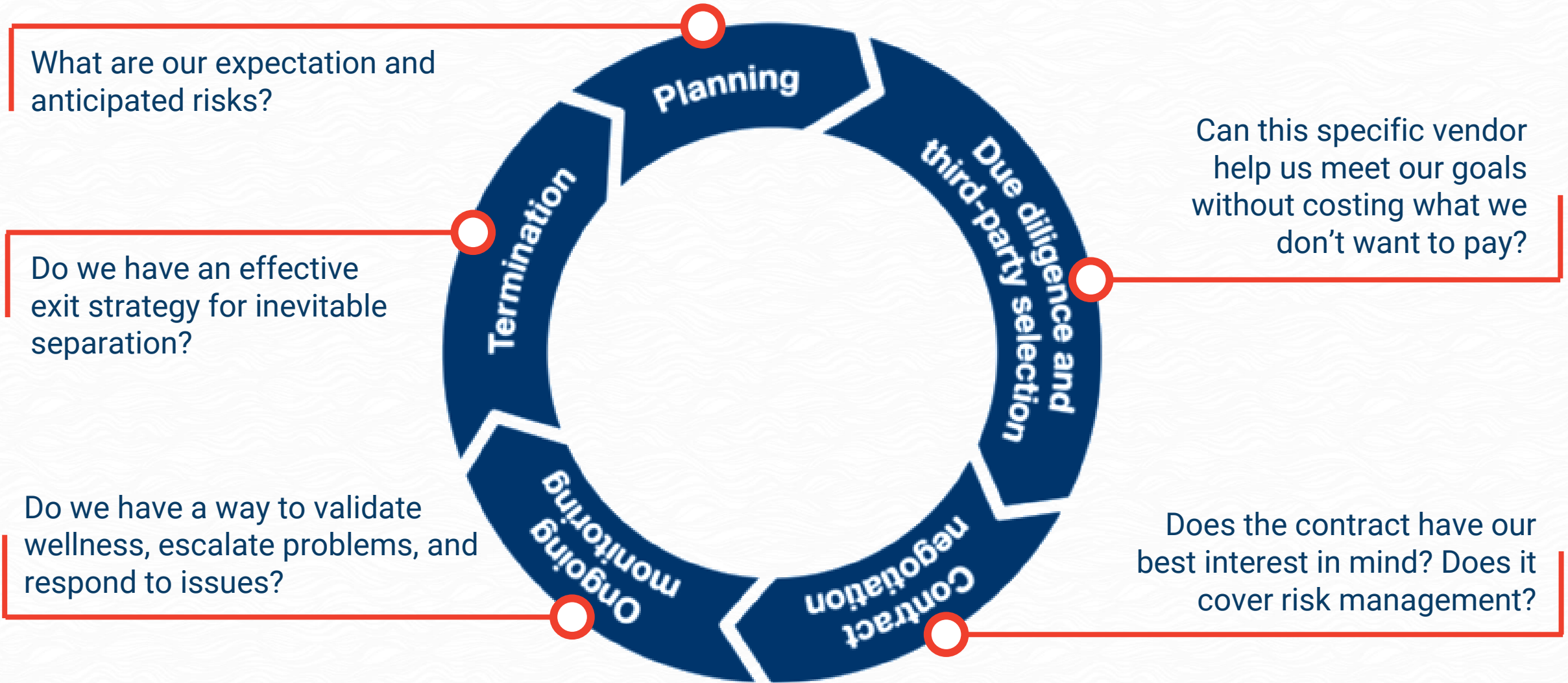
Finalized: 06/06/2023



WATCH THE RECORDING

Tandem.App/TPRM-Webinar-Recording

THIRD-PARTY RELATIONSHIP LIFECYCLE





Subcontractor

individual or business that contracts to perform part (or all) of the obligations of another's contract



Bank Guidance says to look at:

- Volume and types of subcontracted activities
- Degree of reliance on subcontractors
- Geographic location of subcontractors
- Dependence on Single Subcontractor
- Third party's own TPRM process

Credit Union Guidance says to:

Identify subcontractors and understand the purpose and function of each. Further due diligence may be required if they play a critical role in providing the proposed service.

Your third parties should be managing their own third parties. Your job is to evaluate how well you think they do that and respond accordingly.

Bank Guidance suggests contracts:

- Require notification of subcontractor use
- Prohibit subcontracting without consent
- Define prohibited subcontractors

Credit Union Guidance suggests contracts:

Address responsibilities of all parties (including subcontractor oversight).

**SUBMIT YOUR
QUESTIONS!**

**We want to
hear from you.**

Use the “Questions” panel to:

- Ask a question
- Send a chat
- Share a story
- Connect with us

If-Then Due Diligence Method

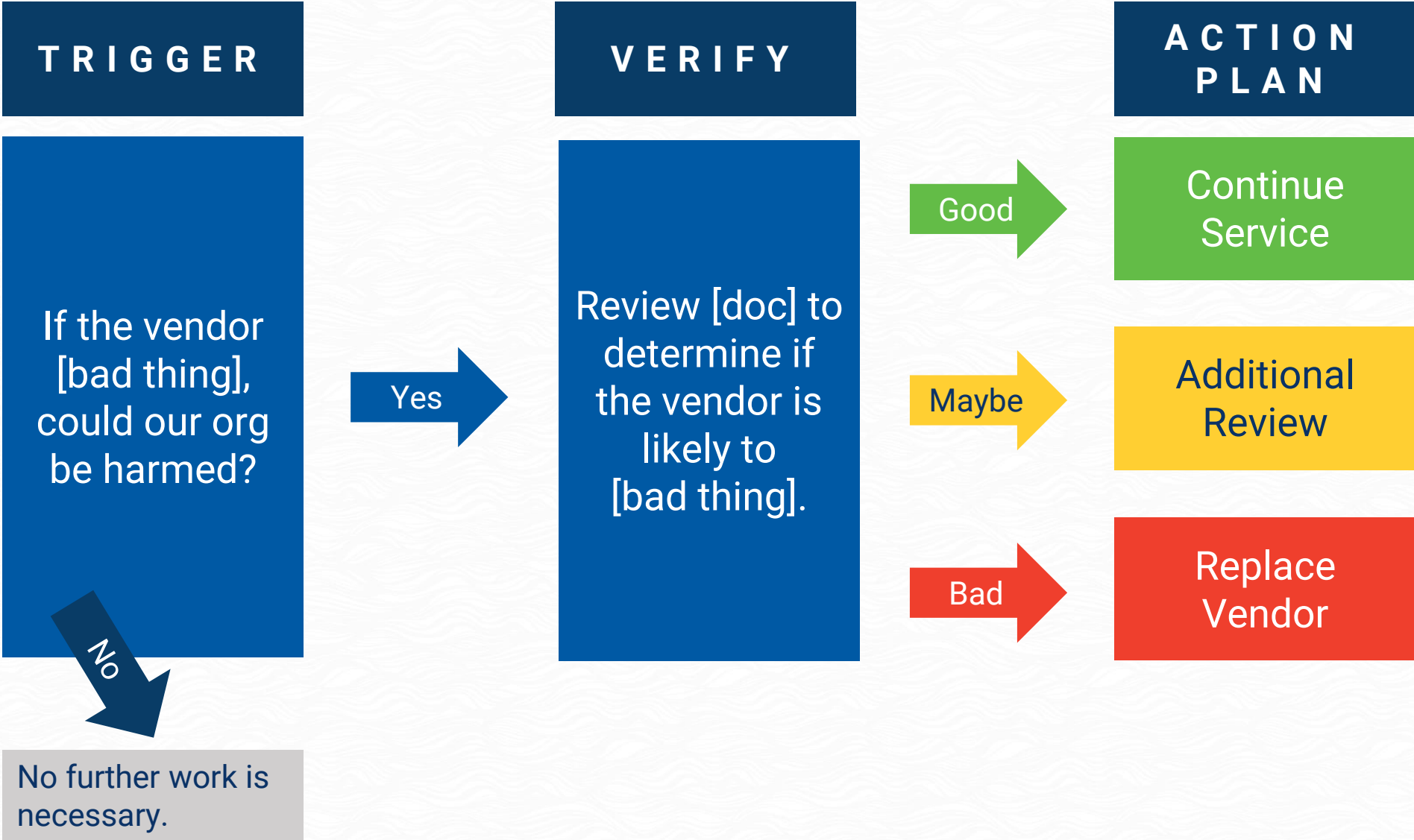


STOP USING THE Bucket Method

#nomorebuckets

Problems created by this method:

1. Unnecessary document exceptions
2. Missed relevant documents



TRIGGER

If the vendor were to have a **subcontractor that suffered a loss of CIA**, could our organization be harmed?

No

No further work is necessary.

Yes

VERIFY

Review your vendor's third party risk program/policy to determine if your vendor is likely to have awareness and jurisdiction over their subcontractors' failures.

Good

Maybe

Bad

1

TANDEM VENDOR MANAGEMENT

If-Then Due Diligence Resource

This resource is designed to provide an example list of due diligence questions and the supporting documents which could be required if you answered the question "yes." The information should be tailored to your unique environment and risks. You can manage this list, along with other questions, using Tandem Vendor Management. Learn more at Tandem.App/Vendor-Management-Software.

DUE DILIGENCE QUESTION	REQUIRED DOCUMENT(S)
Does the vendor perform critical activities for our organization?	SLA
Would our organization be significantly affected if the vendor's services were temporarily unavailable?	BCP Documentation, SLA
Would our organization be significantly affected if the vendor went out of business?	Financial Statements, BCP Documentation, SLA
Does the vendor use subcontractors for critical activities?	
Does the vendor store proprietary data?	
Does the vendor transmit, process or store organization or customer data?	
Does the vendor access proprietary data?	
Does the vendor open or accept data from our organization?	
Does the vendor provide online services to our organization?	
Is the vendor subject to federal or state regulations?	
Does the vendor host a website?	
Does the vendor provide professional services?	

SLA: Service Level Agreement
BCP: Business Continuity Plan
NDA: Non-Disclosure Agreement /
Security Testing: Could include user

Visit Tandem.App for more information.
Tandem, LLC | Copyright © 2020

COLLECTING DUE DILIGENCE DOCUMENTS FROM VENDORS

IF

THEN



THIRD-PARTY RELATIONSHIPS If-Then Due Diligence Resource

[Watch on YouTube](#) | Tandem.App/If-Then

2



3

FOUR FREE TEMPLATES

- [Financial Review](#)
- [SOC Review](#)
- [BCP Review](#)
- [Subcontractor Due Diligence Review](#)



**SUBMIT YOUR
QUESTIONS!**

**We want to
hear from you.**

Use the “Questions” panel to:

- Ask a question
- Send a chat
- Share a story
- Connect with us



Special thanks to Matthew Killough

A Cautionary Tale Case Study

SEC File No. 3-21112


<https://www.sec.gov/litigation/admin/2022/34-95832.pdf>


UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 95832 / September 20, 2022

INVESTMENT ADVISERS ACT OF 1940
Release No. 6138 / September 20, 2022

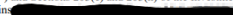
ADMINISTRATIVE PROCEEDING
File No. 3-21112

In the Matter of


Respondent.


ORDER INSTITUTING
ADMINISTRATIVE AND CEASE-AND-
DESIST PROCEEDINGS, PURSUANT TO
SECTIONS 15b AND 21C OF THE
SECURITIES EXCHANGE ACT OF 1934
AND SECTIONS 203(e) AND 203(k) OF
THE INVESTMENT ADVISERS ACT OF
1940, MAKING FINDINGS, AND
IMPOSING REMEDIAL SANCTIONS AND
A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 ("Exchange Act") and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 ("Advisers Act") against  or "Respondent".

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer"), which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15b and 21C of the Securities Exchange Act of 1934 and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order



I'M KIND OF A BIG DEAL



Charged a
\$35,000,000
Fine by the SEC

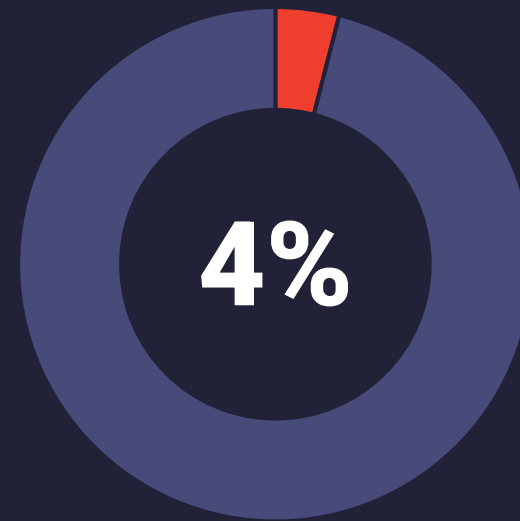


15

MILLION

Customers' Records Exposed

That's equivalent to...



of the American
Population



“[The bank’s] failures in this case are **astonishing**. [...] Customers entrust their personal information to financial professionals with the understanding and expectation that it will be protected, and [the bank] fell **woefully short** in doing so.”

Gurbir S. Grewal
Director of SEC Enforcement Division

VIOLATIONS

The bank willfully violated the Safeguards Rule

because it did not adopt written policies and procedures relating to the safeguarding of customer data, including PII or consumer report information, during the 2016 Data Center Decommissioning and other decommissioning projects.

The bank willfully violated the Disposal Rule

because it maintained devices containing consumer report information but failed to take reasonable measures to protect that information during the 2016 Data Center Decommissioning and other decommissioning projects.





Informed of auctioned un-wiped drives



Charged a **\$35,000,000** Fine by the SEC



"failures in this case are astonishing"





“You are a major financial institution and should be following some very stringent guidelines on how to deal with retiring hardware. Or at the very least getting some kind of verification of data destruction from the vendors you sell equipment to.”

IT Consultant
Oklahoma



Contract with "Moving Company" to decommission 2 primary data centers



Informed of auctioned un-wiped drives



Charged a **\$35,000,000** Fine by the SEC



"failures in this case are astonishing"





AUDIENCE QUESTION

How would you begin your search for a vendor like this?

About 4,500,000 results (0.57 seconds)

4,500,000

Sponsored



Critical Power

<https://www.criticalpower.com>

Data Center Decommissioning - Project Planning & Management

Decommissioning your Data Center? We Reclaim Unwanted Materials! Full Service Solutions. Veteran Owned Company.

Data Center Services

Data Center Relocation & Decom Relocate or Reclaim Data Centers

Site Surveys

By Certified Project Managers Schedule Consultation Today

UPS Inventory

Uninterruptible Power Supplies Request A Quote Today

Generators Inventory

New Used Diesel Natural Gas 30kw and Larger



Contract with "Moving Company" to decommission 2 primary data centers



Informed of auctioned un-wiped drives



Charged a **\$35,000,000** Fine by the SEC



"failures in this case are astonishing"

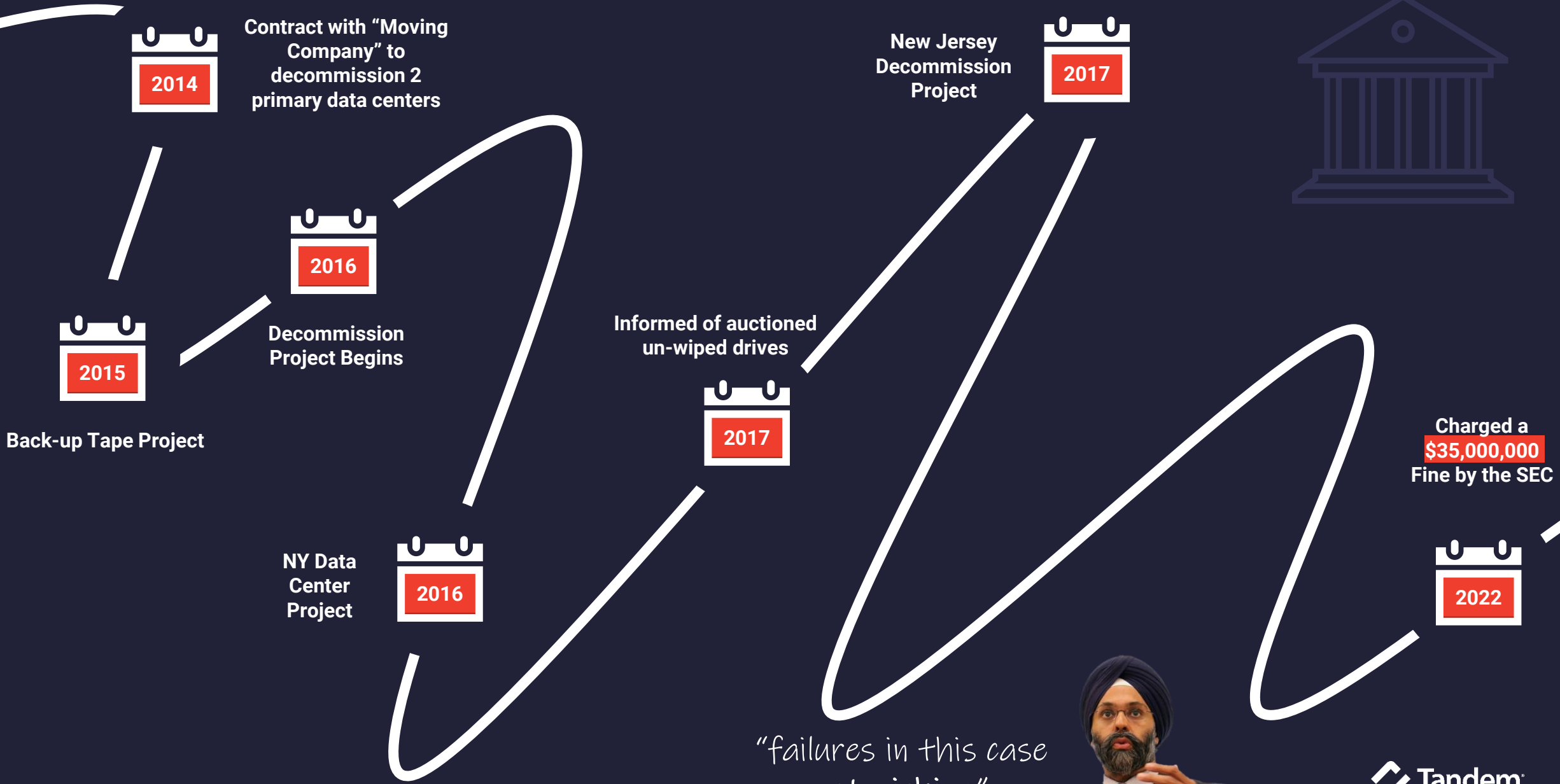


Contract Terms Included

- Moving Company will pick-up, transport and decommission certain devices from data centers
- Devices will be wiped (or degaussed) by IT Corp A (subcontractor) and resold with 60-70 percent of the resale amount going to the bank
- Bank will receive an asset report and a disposition report (inventory and whether they were returned to bank, resold, or destroyed)
- Bank will receive Certificates of Destruction (“CODs”) documenting the destruction of relevant devices



CAUTIONARY TALE



"failures in this case are astonishing"





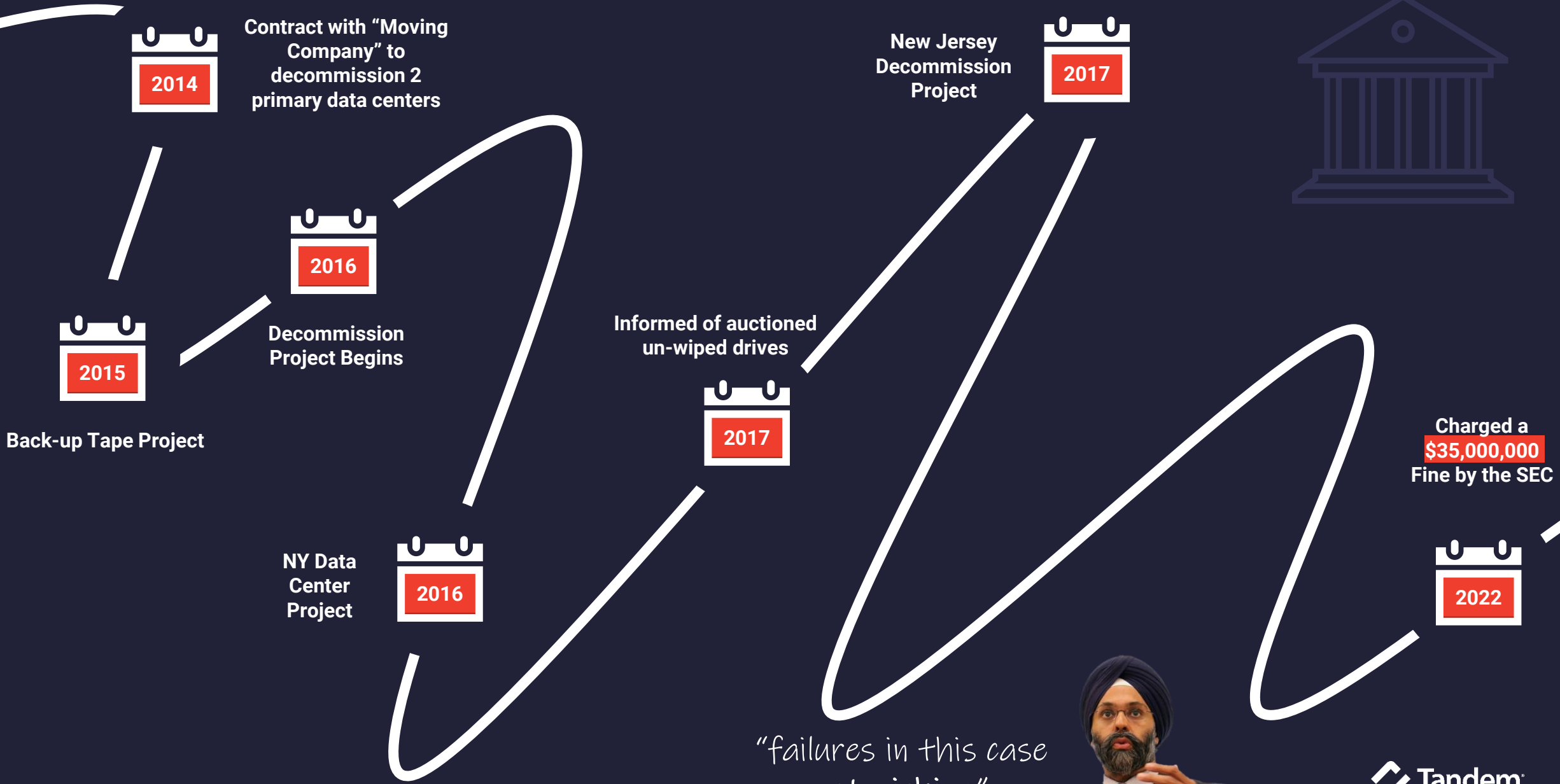
Morgan Stanley

“We are pleased to be resolving this matter. We have previously notified applicable clients regarding these matters, which occurred several years ago, and have not detected any unauthorized access to, or misuse of, personal client information.”

Morgan Stanley Officials

**“The vast majority
of the hard drives
from the
2016 Data Center
Decommissioning
remain missing.”**

CAUTIONARY TALE



"failures in this case are astonishing"





com services.
ertise in,
.” (p2)

sure that a
‘had no
es. **Movina** “is,
y.”



Mov



SITUATION 2: SUB-VENDOR SELECTION

In 2014, **Stanley** approved **Movina** to provide decom services “without the use of a sub-vendor” but then executed a contract where **IT Alvin** is identified as the data wiper. (P3)



SEC EXPRESSED FAILURE (P7)

Stanley's policies and procedures failed to ensure that **Stanley** “reviewed and approved sub-vendors.” Though **Movina** said **IT Alvin** would perform the decom services, **Stanley** “never conducted a review” of IT Alvin or formally approved him “to act as a sub-vendor” for the 2016DCD project.

SOLUTION

P&P that require **the review & approval of subcontractors** (especially for critical services).

IT Alvin



peacock

E
Alvin who
everything in a

anything **IT Alvin**
ed the database
he devices were
the database, he
orking with **IT**

es and projects.



SITUATION 4: DIDN'T WATCH THE MONEY

IT Alvin kept his portion of the resale amount (30%-40%) and gave the rest to **Movina**. **Stanley** never got this money like the contract said he would.



SEC EXPRESSED FAILURE (P3)

“It does not appear that [the bank] ever requested or received the remainder of the resale amount” from **Movina**.

SOLUTION

Assign a champion to know everything about a critical outsourced project.

SITUATION 5: SUB-VENDOR CHANGED

Movina stopped working with **IT Alvin** and began working with **IT Benny** without notifying **Stanley**. **IT Benny** was never vetted by **Stanley** and was never approved as a vendor or sub-vendor for this decommissioning. (P4)



SEC EXPRESSED FAILURE (P7)

Stanley's "policies and procedures were not reasonably designed to ensure that [the bank] was aware of a change in the sub-vendor used" by **Movina**.

SOLUTION

P&P that require the review & approval of subcontractors. Put it in the contract.



SITUATION 6: SERVICE CHANGED

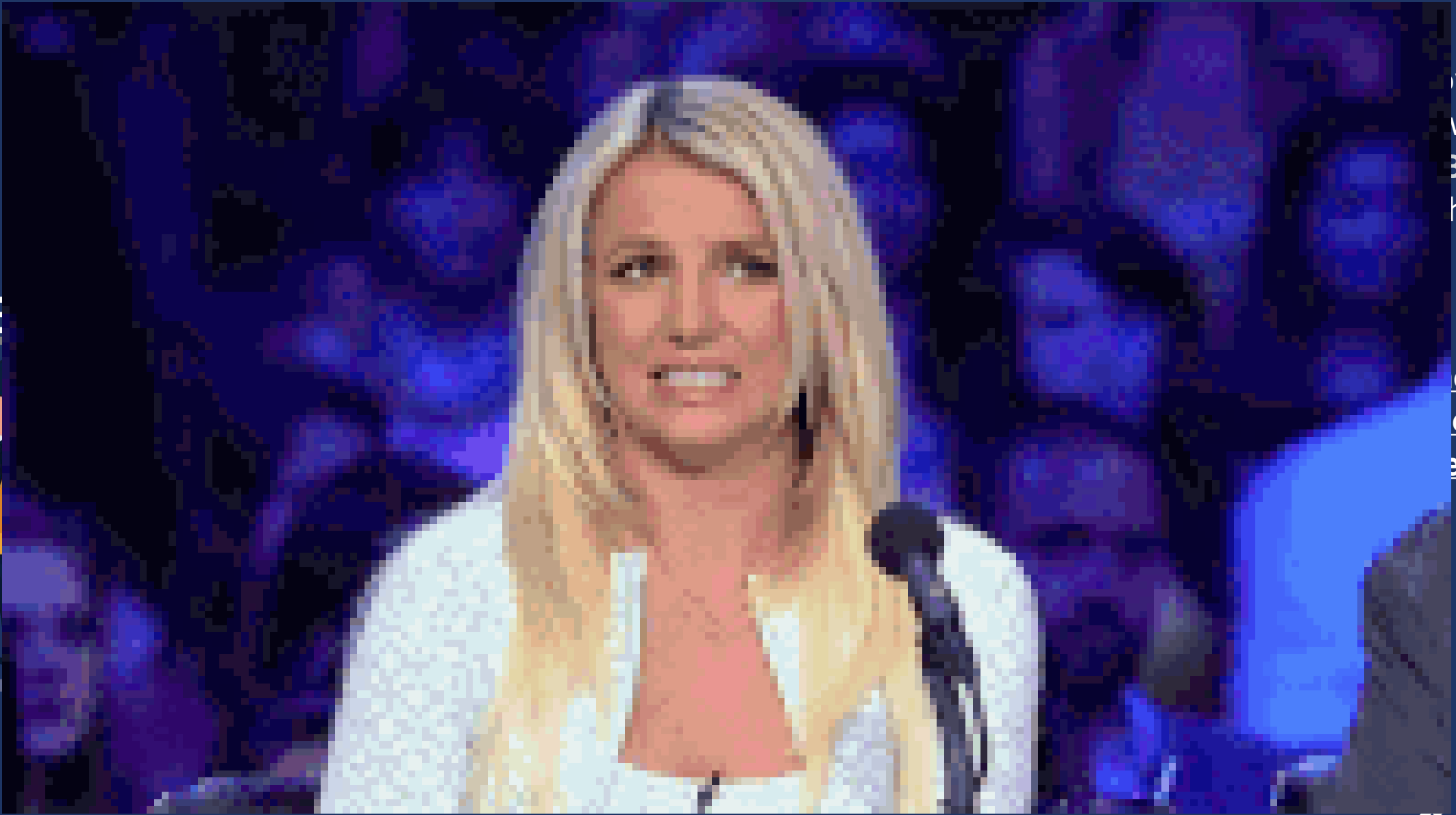
Movina asked IT Benny to bid on hard drives that **Stanley** was selling at auction, when in reality, **Movina** didn't attempt to sell to anyone but IT Benny. **Movina** didn't ask IT Benny to perform data destruction (even though he could). **Movina** led IT Benny to believe the devices *had already been wiped*. So, IT Benny assumed possession and sold the devices down stream.

SEC EXPRESSED FAILURE

n/a

SOLUTION

P&P that require vendors to be trustworthy.



IT E



oving
with
Benny.
h the

enting
ed
e chain



SITUATION 8: DID NOT READ DOCUMENTS

IT Benny provided Certificates of Indemnification (COIs) which showed that they assumed possession of the devices. “Those COIs contained the logo and letterhead” of IT Benny. **Movina** emailed the certificates to **Stanley** but called them CODs. **Stanley** *did not review* the COIs.

SEC EXPRESSED FAILURE (P4)

If **Stanley** had reviewed the COIs, it would have been clear that **Movina** “was using a sub-vendor that had not been vetted by [the bank] and that the hard drives were not being wiped of data.”

SOLUTION

Read documents sent to you for verification.

Stanley

Morgan



SITUATION 9: DELAYED INVESTIGATION

As early as March 2017, part of **Stanley** (maybe **Morgan**) became aware of the problems **Movina** had with record maintenance but didn't trigger a broader investigation until notified by the Oklahoma consultant in October.

SEC EXPRESSED FAILURE (#25 #26)

Stanley's "policies and procedures failed to provide for sufficient monitoring of [Movina's] performance." Leading to several more months of **Movina** misrepresenting her services.

Stanley's iRespond system that requires personnel to immediately report suspected/confirmed incidents "did not specifically require that concerns about a vendor be investigated. Reasonably designed policies and procedures would have expressly required that."

SOLUTION

P&P that require **immediate investigation of suspicious vendors.**

Movina

Stanley



SITUATION 10: INACCURATE RISK ASSESSMENT

Stanley continued to approve **Movina** as a vendor through annual vendor approval documents, with **Movina's** risk rating decreasing between 2015 and 2017.

SEC EXPRESSED FAILURE (#24)

Stanley's risk assessment process "failed to note" important and known information about **Movina**.

- 5/29/15 - Risk Level: Moderate | No mention of sub-vendor | Acknowledged "security program is not independently assessed leading to potential gaps in security, breaches, and non-compliance with policies and regulatory requirements."
- 8/1/16 - Risk Level: Moderate | Expressly states no material sub-vendors | Omits previous acknowledgement
- 5/11/17 - Risk Level: Low | Expressly states no material sub-vendors | Omits previous acknowledgement

SOLUTION

Less siloing between vendor management duties.



Stanley



SITUATION 11: POORLY DEFINED RISK

Stanley's P&P did not express that projects related to decommissioning devices with PII and consumer report info should be considered high risk.

SEC EXPRESSED FAILURE (#20)

Stanley “failed to adopt written policies and procedures that identified the high level of risk associated with the decommissioning of devices. Given that many of [the bank’s] data bearing devices likely contained PII and consumer report information, and that many of the devices remained unencrypted, all decommissioning projects should have been catalogued as high risk.”

SOLUTION

Understand the definition of high risk includes things dealing with sensitive customer data.

Movina

Stanley



SITUATION 12: PAID INCOMPLETE CONTRACT

Throughout the 2016DCD project, **Movina** invoiced **Stanley** – and was paid – for collecting, shipping, and wiping/degaussing the hard drives.

SEC EXPRESSED FAILURE (P4)

Stanley paid **Movina**, “even though no wiping or degaussing services were provided” after **Movina** stopped working with IT Alvin.

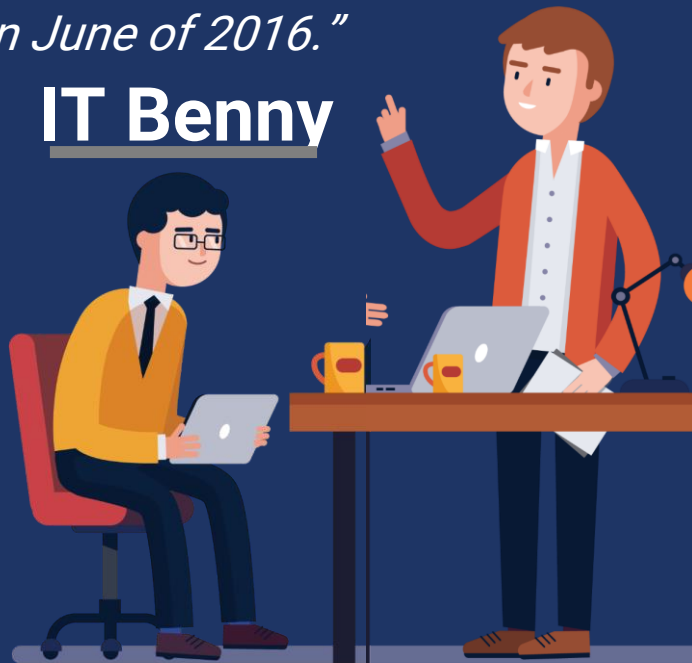
SOLUTION

Follow your contracts and only pay for services received.

"I can confirm that we did send this load of tapes for secure waste to energy incineration. Although that lot # is not the lot # we used. They were processed 'Confidential Material' in June of 2016."

IT Benny

Stanley



SITUATION 13: NO DOC OF DESTRUCTION

Stanley emailed IT Benny on 1/19/18 to ask if IT Benny could confirm the disposal of "3k lbs of tapes" from 18 months prior. IT Benny responded...

SEC EXPRESSED FAILURE (P4 P8)

Stanley's belief in the destruction of tapes without any unauthorized access "hinges on this email. [The bank] has no other verification or documentation that these tapes were destroyed."

For the 8,000 tapes delivered to IT Benny, **Stanley** "never received a COD—in fact [the bank] didn't even know that the tapes had been sent to [IT Benny...] another unapproved sub-vendor."

SOLUTION

Contract with a vendor who can provide the service you need.

SITUATION 14: IGNORED POLICIES

In a 2015 engagement with **Movina**, 32,000 backup tapes from **Stanley** were taking to **IT Alvin** for shredding. While they were shredded and provided CODs, the destruction did not meet policy requirements for backup tapes (shorter window from removal to destruction, specifications on the devices used to wipe data and random sampling to ensure destruction).

SEC EXPRESSED FAILURE (P8)

Stanley “failed to implement and monitor compliance with its own policies and procedures relating to the destruction of back-up tapes.” **Stanley** never inspected the equipment used to destroy those tapes, the tapes were not destroyed within 24 hours, **Stanley** never did random sampling, and the COD from **IT Alvin** did not specify the method by which the tapes were destroyed.

SOLUTION

Know and follow your P&P.



Movina

Stanley



SITUATION 15: DIDN'T ENFORCE DOCUMENTATION

2016 NYC DCD by **Movina**. **Stanley** “does not have records sufficient” to identify the number or types of devices or what data they may have contained, and “does not have CODs for any of those devices.” (P5)

2017 NJ Decom by **Movina**. Employee that hired **Movina** “did not go through the required channels”. The COD for the 61 servers “did not meet standards” from **Stanley's** policies to identify each of the 244 hard drives. There was confusion about serial numbers, that cannot be confirmed because of destruction. (P5)

SEC EXPRESSED FAILURE (P5)

Between 2015 and 2017, [Movina] was engaged for additional decom projects for which **Stanley** “did not comply with its internal policies or procedures and/or maintain documentation sufficient to confirm that its policies were followed.”

SOLUTION

Know and follow your P&P. Maintain documents that prove it.



Still at Large

In June 2021, **Stanley** obtained another 14 of the missing hard drives from a downstream purchaser.

Forensics show 13 of the devices contained a total of at least 140 pieces of customers PII.

“The vast majority of the hard drives from the 2016DCD remain missing.”
(P5)

O
W

S

Th
20
af

In
th
St
th

S

St

in
fa

S

M



Lessons Learned

Where they missed the mark:

How we can get it right:

Selected a vendor without experience.

Did not get necessary documentation and hinge trust on an email message.

Paid for services that were not received.

Did not review the Certificates.

Did not identify decommissioning devices with PII and consumer report info as high risk.

Allowed a subcontractor to be part of a contract with formal review or approval.

Unknowingly allowed a new sub-vendor to access their data.

Did not review the monitoring database provided.

Unknowingly allowed a vendor to modify the service being provided.

Did not investigate the vendor after noticing record maintenance issues.

Didn't follow their own policies for moving hard drives.

Did not ensure vendor followed policies.

Did not comply with their own policies nor maintain documentation.

Did not monitor encryption. Did not get documentation of destruction or chain of custody.

Risk assessments did not reflect truth about the vendor.

Didn't notice they were not being paid.

Common Sense

- P&P that require vendors to be experienced.
- Use a vendor who can provide the service you need.
- Follow your contracts and only pay for services received.
- Read documents sent to you for verification.
- Sensitive customer data = High Risk

Make Policies

- that require the review & approval of subcontractors & put it in the contract
- that require monitoring of critical services and projects.
- that require immediate investigation of suspicious vendors.

Follow Your Policies

- Know them
- Follow them
- Document to prove you followed them

Designate a Responsible Party

- Less siloing between vendor management duties.
- Assign a champion to know everything about a critical outsourced project.

VIOLATIONS

The bank willfully violated the Safeguards Rule

because it did not adopt written policies and procedures relating to the safeguarding of customer data, including PII or consumer report information, during the 2016 Data Center Decommissioning and other decommissioning projects.

The bank willfully violated the Disposal Rule

because it maintained devices containing consumer report information but failed to take reasonable measures to protect that information during the 2016 Data Center Decommissioning and other decommissioning projects.



**SUBMIT YOUR
QUESTIONS!**

**We want to
hear from you.**

Use the “Questions” panel to:

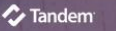
- Ask a question
- Send a chat
- Share a story
- Connect with us

RECAP

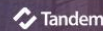
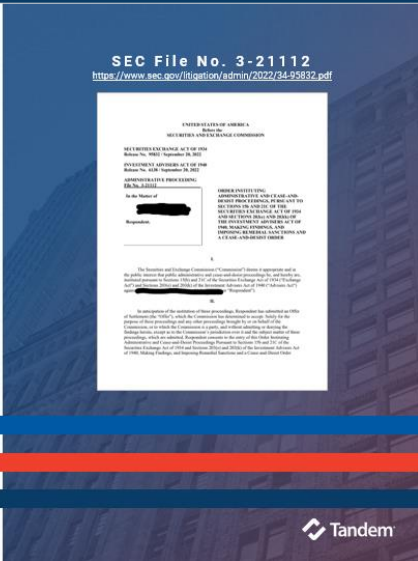
Subcontractors Guidance



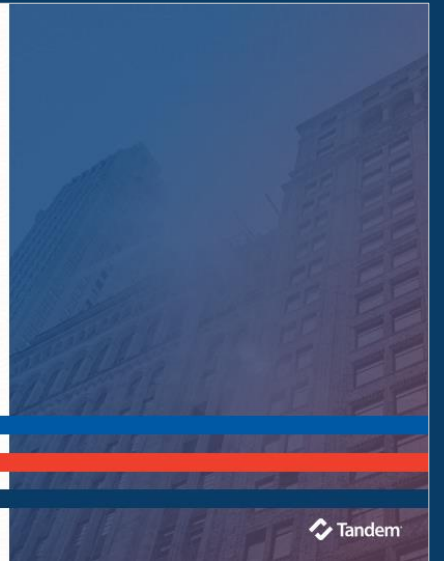
If-Then Due Diligence Method



A Cautionary Tale Case Study



Lessons Learned



BONUS CONTENT

Tandem Vendor Management



COMPLETE THE SURVEY
Answer "Yes" on Question 4



VISIT OUR WEBSITE
Tandem.App/Demos





Tandem.App/KEYS

THANKS FOR JOINING

A Case Study of What NOT to Do in Vendor Management

Leticia Saiid, Security+
Chief of Staff & Chief Learning Officer
[LinkedIn.com/in/LeticiaSaiid](https://www.linkedin.com/in/LeticiaSaiid)



Remember to complete the survey!