

LEVEL UP

Leticia Saiid

Saving Your Customers Through Due Diligence

Cybersecurity



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

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.



2



Leticia (Letice) Saiid

Security+
Chief of Staff & Chief Learning Officer



3

About Me

SOME THINGS I LOVE

Piano



Parenting



Personality Tests



Fiona



Puzzles



4

Agenda

HERE'S THE PLAN

- FFIEC Expectations
- Due Diligence Methods
- A Case Study



5

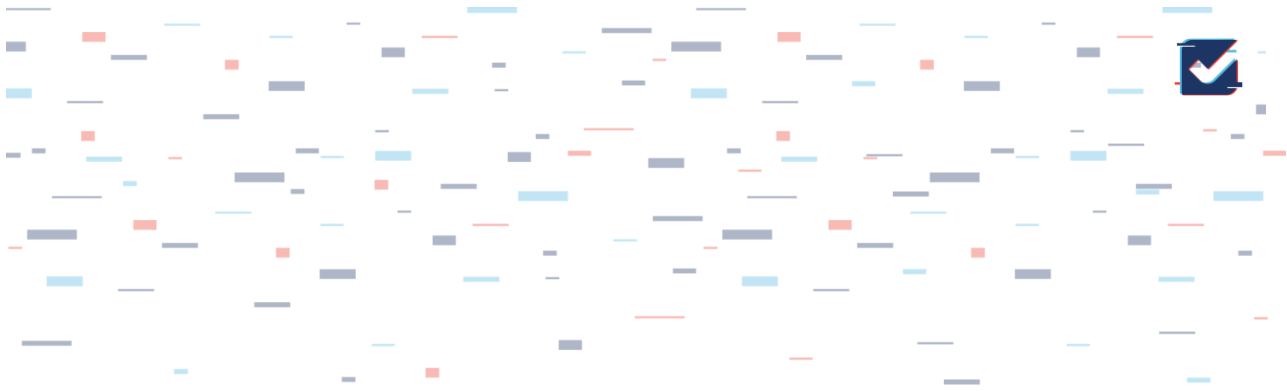


AUDIENCE QUESTION



Are you outsourcing due diligence determination, gathering, and/or reviewing?

6



Regulatory Expectations

FOR VENDOR MANAGEMENT AND DUE DILIGENCE

7


[IT BOOKLETS](#)
[IT WORKPROGRAMS](#)
[GLOSSARY](#)
[FFIEC HOME](#)
 

INFORMATION SECURITY

Home / IT Booklets / Information Security / II Information Security Program Management / IIC Risk Mitigation / IIC.20 Oversight of Third-Party Service Providers

Information Security Booklet Contents

- Introduction
- I Governance of the Information Security Program
 - I.A Security Culture
 - I.B Responsibility and Accountability
 - I.C Resources
- II Information Security Program Management
 - II.A Risk Identification
 - II.A.1 Threats
 - II.A.2 Vulnerabilities
 - II.A.3 Supervision of Cybersecurity Risk and

II.C.20 Oversight of Third-Party Service Providers

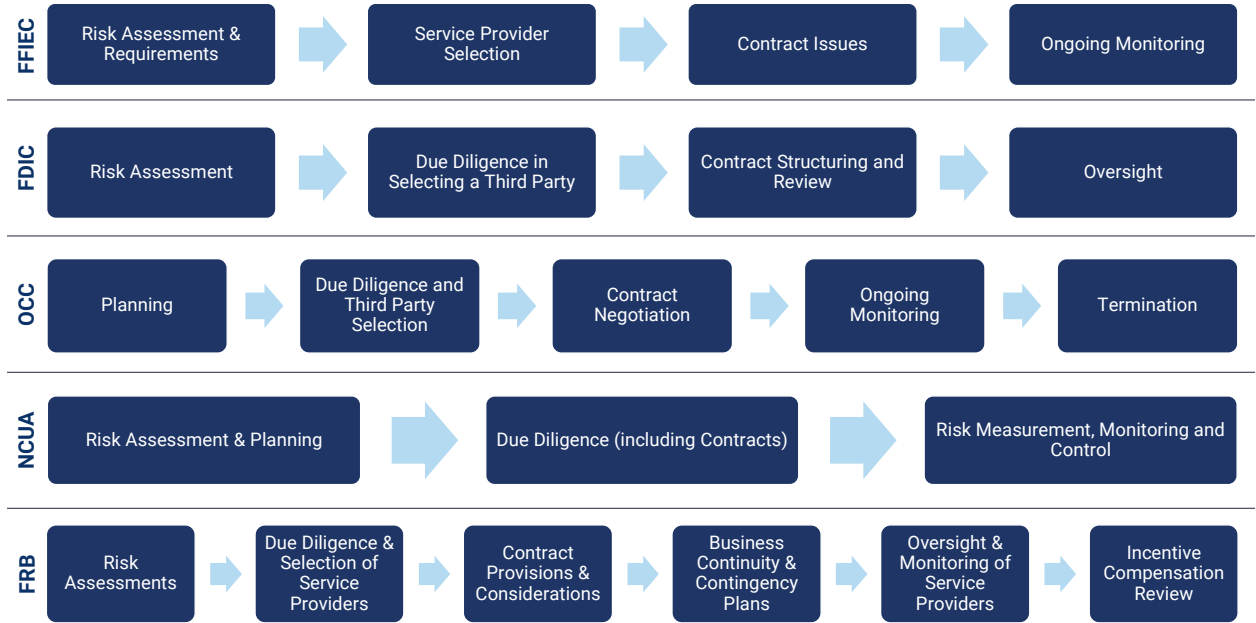
Action Summary

Management should oversee outsourced operations through the following:

- Appropriate due diligence in third-party research, selection, and relationship management.
- Contractual assurances for security responsibilities, controls, and reporting.
- Nondisclosure agreements regarding the institution's systems and data.
- Independent review of the third party's security through appropriate reports from audits and tests.
- Coordination of incident response policies and contractual notification requirements.
- Verification that information and cybersecurity risks are appropriately identified, measured, mitigated, monitored, and reported.

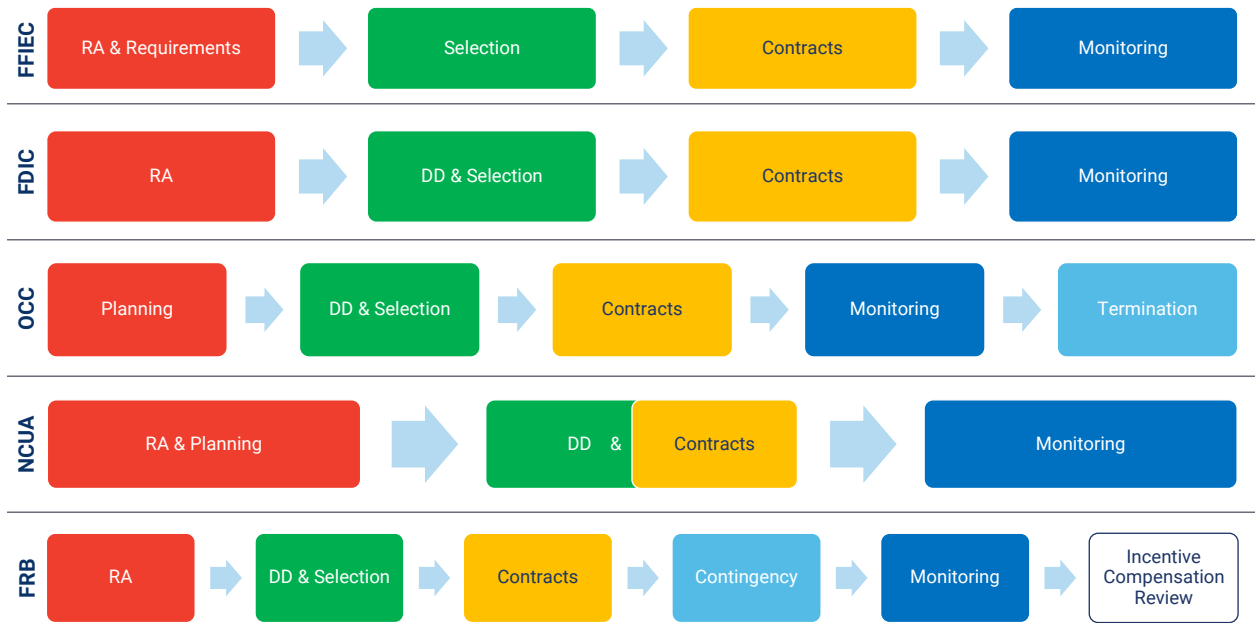
8

WHAT THE GUIDANCE SAYS



9

WHAT THE GUIDANCE SAYS



10

Vendor Risk Management Process

THE ULTIMATE




11


Did you know?

Doing Your Due Diligence

Due diligence has been used since at least the mid-fifteenth century in the literal sense "requisite effort." Centuries later, the phrase developed a legal meaning, namely, "the care that a reasonable person takes to avoid harm to other persons or their property"; in this sense, it is synonymous with another legal term, *ordinary care*. More recently, *due diligence* has extended its reach into business contexts, signifying the research a company performs before engaging in a financial transaction. This meaning may also apply to individuals: people are often advised to perform their *due diligence* before buying a house, signing a loan, or making any important purchase.



DEFINITION



12



Gathering Methods

FOR VENDOR MANAGEMENT DUE DILIGENCE

13



AUDIENCE QUESTION



How do you know which vendors need to provide which documents?

14



STOP USING THE Bucket Method

#emptythebucket

Problems created by this method:

1. Unnecessary document exceptions
2. Missed relevant documents



15

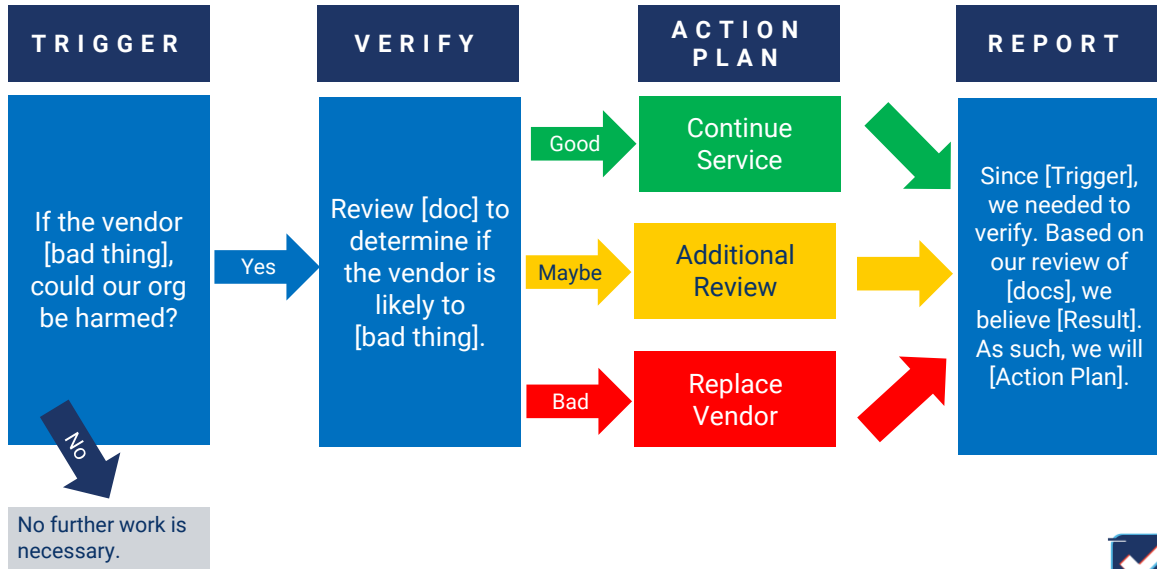


Channel your inner child and ask “Why?”



16

GATHERING METHODS



<https://tandem.app/blog/a-more-accurate-method-for-collecting-due-diligence-documents-from-third-parties>

Review Template: BCP
A BCP Review template is included with Tandem Vendor Management. This article provides further explanation into the concepts behind each question on the BCP Review.

Review Template: Financial Statement
Review this article to learn how to utilize the Financial Statement Review template in Vendor Management!

Review Template: FinTech
A FinTech Review template is included with Tandem Vendor Management. This article provides further explanation into the concepts behind each question on the FinTech Review.

Review Template: Security Testing
A Security Testing Review template is included with Tandem Vendor Management to help organizations review a vendor's results of security testing.

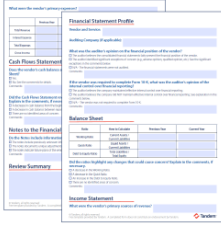
Review Template: SOC Report
A SOC Report review template is included with Tandem Vendor Management. This article provides further explanation into the concepts behind each question on the SOC Report Review.

Review Template: Subcontractors
A Subcontractors Review template is included with Tandem Vendor Management. This article provides further explanation into the concepts behind each question on the Subcontractors Review.

Secure · tandem · app

Knowledge Base

FINANCIALS



For Non-Subscribers
<https://tandem.app/financial-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=1342>

3RD PARTY DD



For Non-Subscribers
<https://tandem.app/soc-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4128>

SOC REPORT



For Non-Subscribers
<https://tandem.app/soc-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4128>

BCP



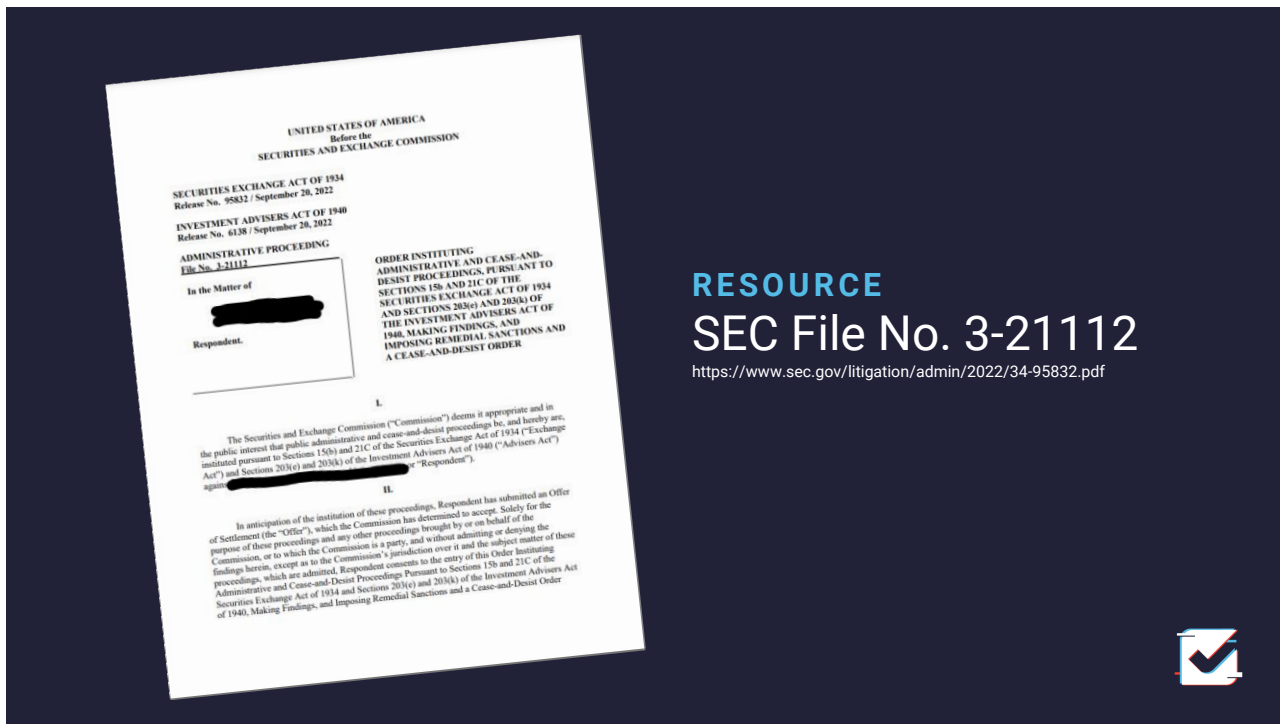
For Non-Subscribers
<https://tandem.app/bcp-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4144>

19

A Court Room Case Study

20



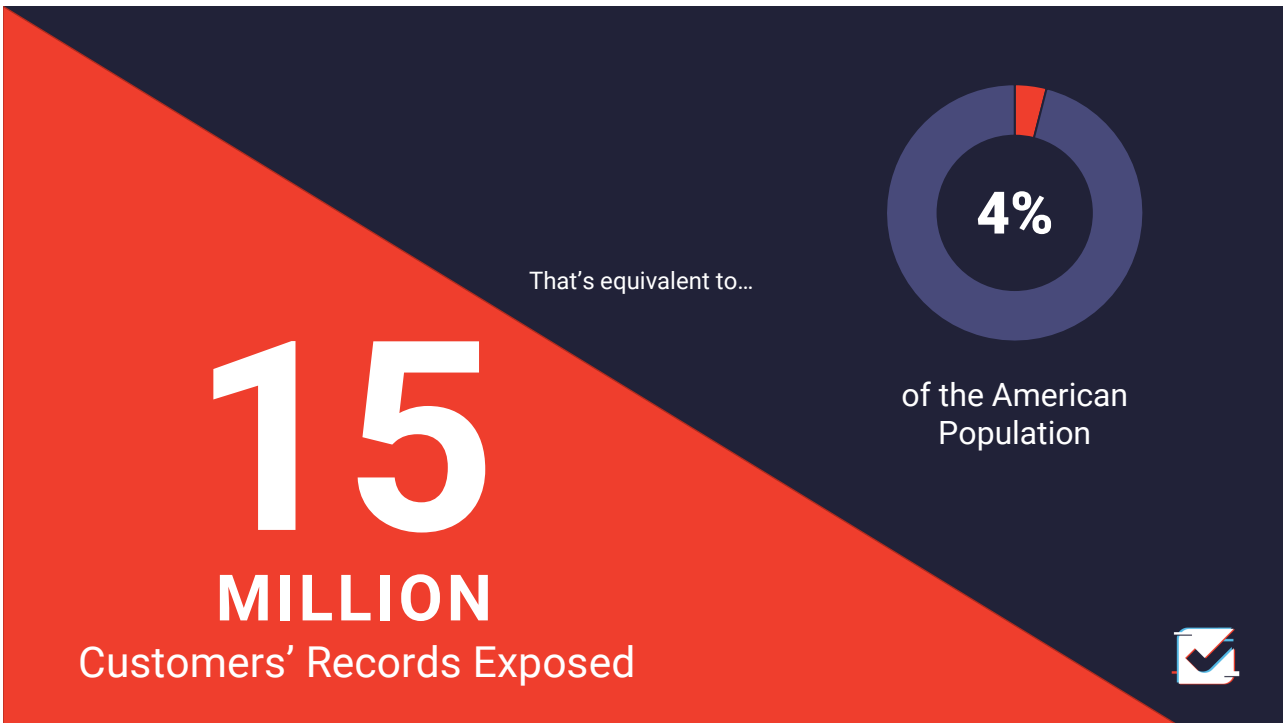
21



22



23



24



“[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



25

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.



SEC File No. 3-21112

26

CAUTIONARY TALE

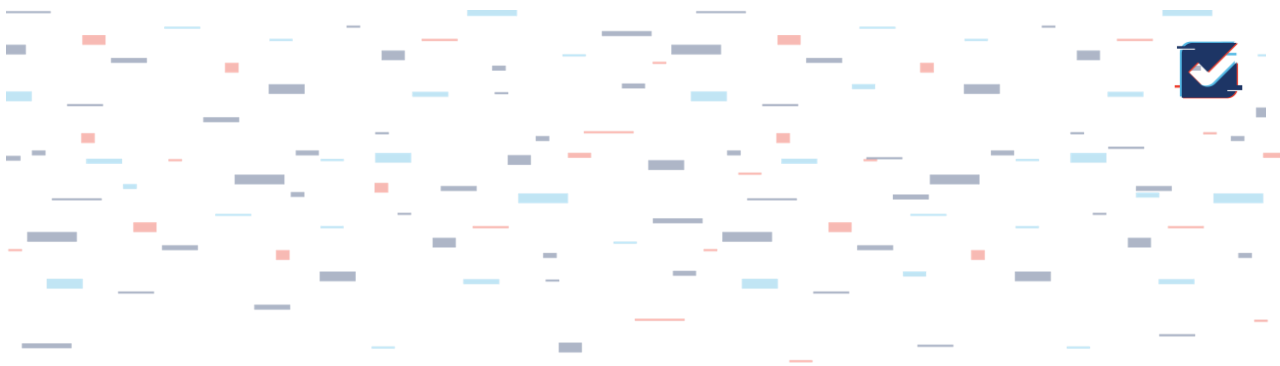
2014 Contract with "Moving Company" to decommission 2 primary data centers

2017 Informed of auctioned un-wiped drives

2022 Charged a **\$35,000,000** Fine by the SEC

"failures in this case are astonishing"

29



AUDIENCE QUESTION

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

30

Google search results for "data center decommission company". The search bar shows the query and the number of results: "About 4,500,000 results (0.5 seconds)". A red circle highlights the number of results, with a red arrow pointing to a large red "4,500,000" displayed on the right. Below the search bar are navigation tabs for News, Images, Maps, Shopping, Videos, Books, Flights, and Finance. The first sponsored result is from Critical Power, with the URL <https://www.criticalpower.com>. The ad title is "Data Center Decommissioning - Project Planning & Management" and the text reads: "Decommissioning your Data Center? We Reclaim Unwanted Materials! Full Service Solutions. Veteran Owned Company." Below the ad are sections for "Data Center Services", "Site Surveys", "UPS Inventory", and "Generators Inventory".

31

CAUTIONARY TALE

2014: Contract with "Moving Company" to decommission 2 primary data centers

2017: Informed of auctioned un-wiped drives

2022: Charged a \$35,000,000 Fine by the SEC

"failures in this case are astonishing"

The timeline is set against a dark blue background with a white wavy line connecting the events. A calendar icon is used for each year. A classical building icon is in the upper right, and a man in a turban is in the lower right. A checkmark icon is at the bottom right.

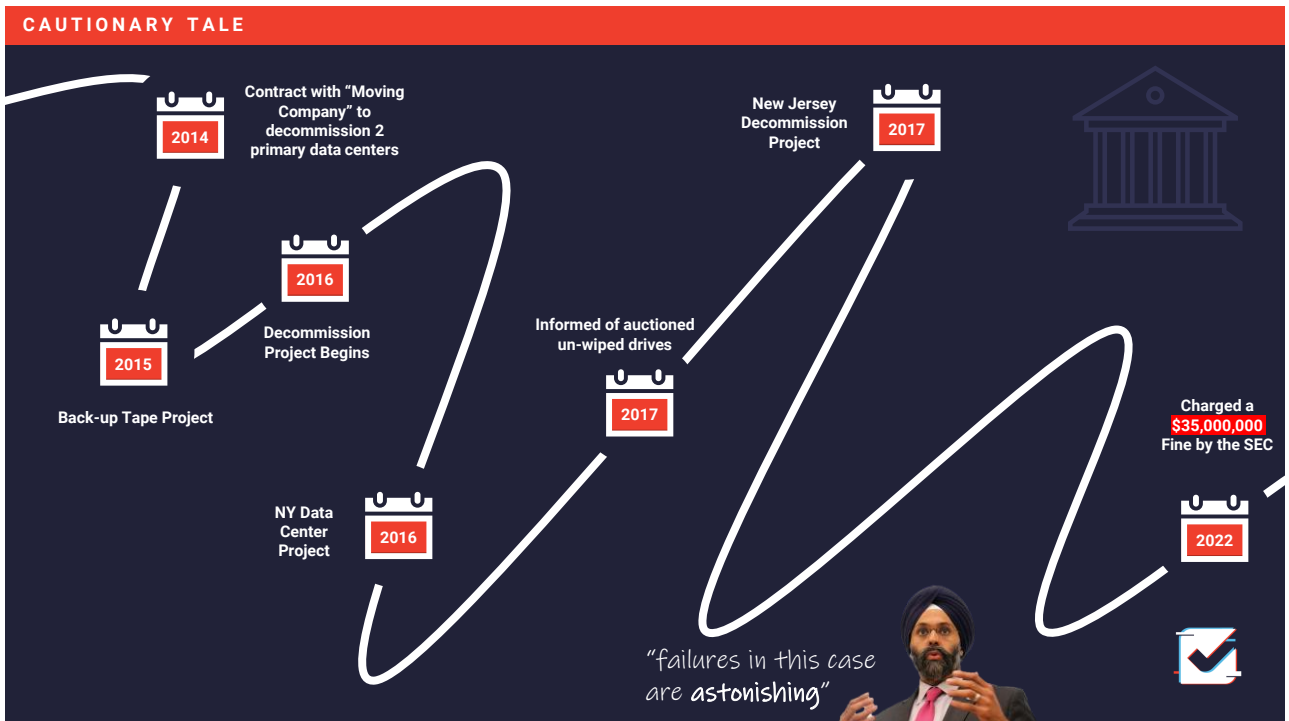
32

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



33



34



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

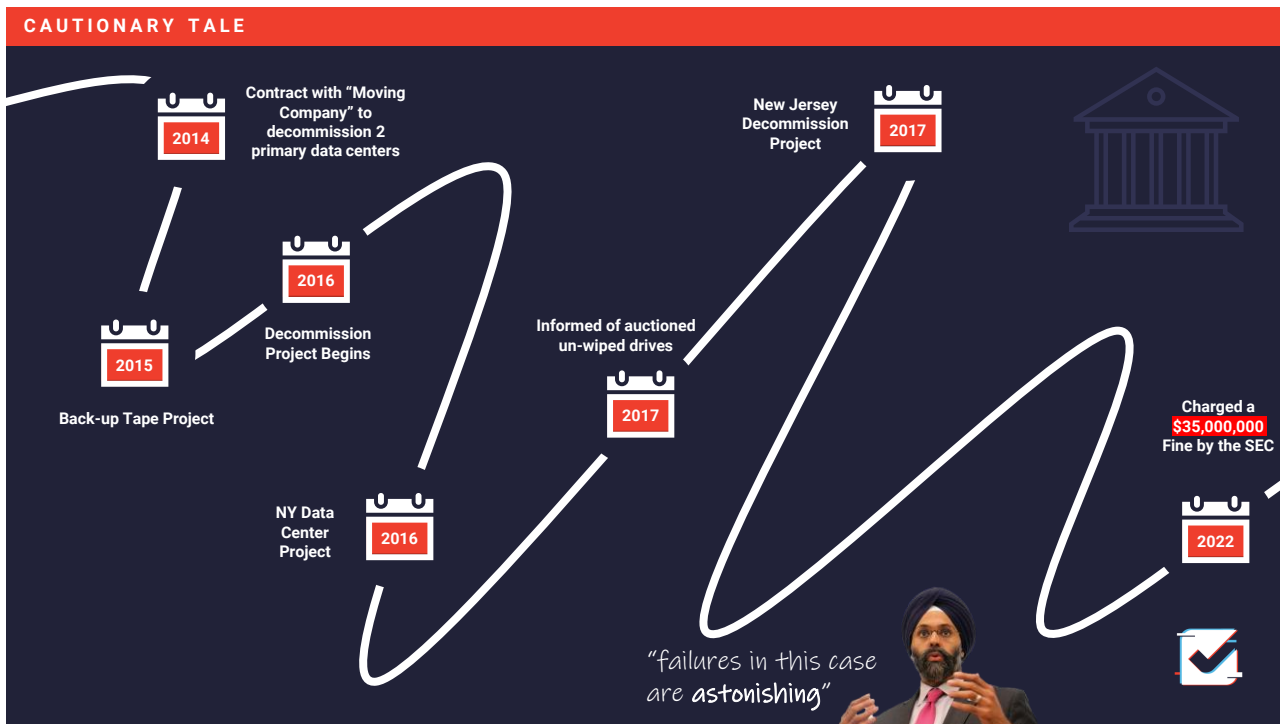
35

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

Section 11

36





37



38

ASTONISHING FAILURES



Movina

Stanley



SITUATION 1: VENDOR SELECTION

In 2014, **Stanley** approved **Movina** to provide decom services. Though **Movina** “had no experience with, or expertise in, providing such data decommissioning services.” (p2)

SEC EXPRESSED FAILURE (P7)

Stanley’s “Policies and procedures failed to ensure that a qualified vendor was used” for decom. **Movina** “had no capability” to provide the required decom services. **Movina** “is, and has always been, strictly a moving company.”

SOLUTION

Have P&P that require selected vendors to be experienced in the service they will provide.



39

ASTONISHING FAILURES

Movina

Stanley

IT Alvin



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

Have P&P that require the review and approval of sub-vendors providing critical services.



40

ASTONISHING FAILURES

SITUATION 3: UNUSED RESOURCE

For a while, **Movina** delivered devices to **IT Alvin** who collected, wiped, released and documented everything in a database directly accessible by **Stanley**.



SEC EXPRESSED FAILURE (P3)

Stanley had access to see the status of everything **IT Alvin** was doing, yet “No one at [the bank] monitored the database or had any direct contact [...] to ensure that the devices were properly handled.” If **Stanley** was monitoring the database, he would have noticed when **Movina** stopped working with **IT Alvin**.

SOLUTION

Have P&P that describe how you will stay informed of the progress of projects performed by vendors.



41

ASTONISHING FAILURES

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 P7)

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

Stanley “did not have written policies and procedures relating to the resale of old or decommissioned devices. [This absence] created confusion that further contributed to the data breach.”

SOLUTION

Have P&P that define what happens when old or decommissioned devices are resold.



42

ASTONISHING FAILURES

SITUATION 5: CONTRACT BREACH
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

Have P&P that ensure you will be informed with a critical sub-vendor is changed.



43

ASTONISHING FAILURES

SITUATION 6: CONTRACT BREACH
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

Hire trustworthy vendors and require frequent updates.



44

ASTONISHING FAILURES

SITUATION 7: IGNORED POLICIES

Stanley's P&P included heightened requirements for moving hard drives. Yet, **Stanley** transported hard drive shelves with drives in place, confirmed by witnesses, **Movina** and IT Benny. IT Benny also sold the shelves to another purchaser with the drives still present. (P9)

SEC EXPRESSED FAILURE (P8)

Stanley “did not follow its own requirements for documenting the destruction of data [...] contained on decommissioned devices. [Stanley] did not obtain CODs, or document the chain of custody for devices” throughout the decom process.

SOLUTION

When a vendor will be taking action on your behalf, review related policies to ensure they meet your organizations expectations.



45

ASTONISHING FAILURES

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

When you receive documentation from a vendor that is for verification purposes, open and read the documents.



46

ASTONISHING FAILURES

StanleyMorgan

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

Have P&P that require immediate reporting/investigation of concerns surrounding a past, current, or future vendor. 

47

ASTONISHING FAILURES

MovinaStanley

SITUATION 10: INCOMPLETE RISK ASSESSMT

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**.

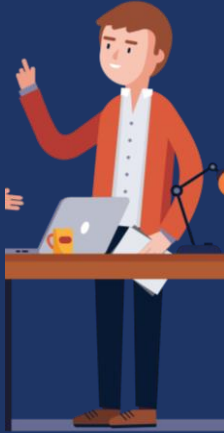
- 5/29/15 - Risk Level: Moderate | No mention of sub-vendor | Acknowledged "security program is not independently assessed leading to potential gaps in security, breaches, and non-compliance with policies and regulatory requirements."
- 8/1/16 - Risk Level: Moderate | Expressly states no material sub-vendors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

SOLUTION (IDEA)

Less siloing between vendor management duties. 

48

ASTONISHING FAILURES

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 MSSB 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

Consider any project to do with protecting customer data to be high risk.



49

ASTONISHING FAILURES

MovinaStanley**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

Confirm service is provided as contracted prior to paying a contract.



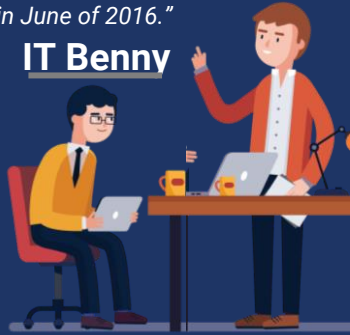
50

ASTONISHING FAILURES

"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 (IDEA)

Require COD's or documentation that no destruction has occurred to be delivered to you on some frequency. AND If possible, contract directly with the vendor providing your service.



51

ASTONISHING FAILURES

IT Alvin

Movina

Stanley



SITUATION 14: IGNORED POLICIES (2)

In a 2015 engagement with **Movina**, 32,000 backup tapes from **Stanley** were taken 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

Assign a champion to ensure vendors follow your organization's expectations/policies.



52

ASTONISHING FAILURES

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

Assign a champion to ensure vendors follow your organization's expectations/policies.



53

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)

54



Surprise! One More Section

55

Wide Area Application Services (WAAS) Devices

SITUATION 16: DROPPED THE ENCRYPTION BALL

Though equipped, **Stanley** “failed to “turn-on” the encryption capability until 2018.” And because of a manufacturing flaw, “data that was not overwritten after 2018 remained unencrypted.”

In 2019, **Stanley** decom-ed 500 devices. In Feb. 2020, **Stanley** “realized that there were 4 missing devices” & discovered the encryption issue. In 2021, **Stanley** undertook an inventory of ALL historical branch devices & discovered that “an additional 38 devices could not be located.”

SEC EXPRESSED FAILURE (P6)

Stanley “failed to document the final disposition of the WAAS devices, including CODs and documents evidencing chain of custody. [The bank] also failed to monitor the encryption of data on those branch devices.”

SOLUTION

Do not forsake your documentation nor monitoring.



56



57

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.



SEC File No. 3-21112

58

Vendor Risk Management Process

THE ULTIMATE



59

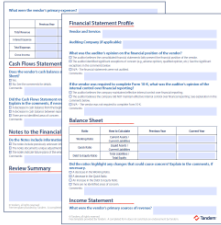
Recap

HERE'S WHERE WE'VE BEEN

- FFIEC Expectations
- Due Diligence Methods
- A Case Study

60

FINANCIALS



For Non-Subscribers
<https://tandem.app/financial-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=1342>

3RD PARTY DD



For Non-Subscribers
<https://tandem.app/soc-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4128>

SOC REPORT



For Non-Subscribers
<https://tandem.app/soc-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4128>

BCP



For Non-Subscribers
<https://tandem.app/bcp-review-pdf>

For VM Subscribers
<https://secure.tandem.app/KnowledgeBaseArticles/Show?id=4144>

61

LEVEL UP

THANKS FOR JOINING!

Saving your Customers Through Due Diligence

Leticia Saiid

Security+, COS/CLO

CoNetrix & Tandem

www.linkedin.com/in/leticiasaiid/



64