International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 07 Issue 07 July 2024

DOI: 10.47191/ijsshr/v7-i07-125 Impact factor- 7.876

Page No: 5716-5745

Nine Cases and Scenarios Involving Retail Financial Compliance

Donald L. Buresh, Ph.D., Esq.
Touro University Worldwide

ABSTRACT: This article discusses retail financial compliance from the perspective of nine cases and scenarios. First, the paper defines financial compliance, a fiduciary, a fiduciary's standard of care, and a broker/dealer. It then describes under what conditions a broker/dealer is a fiduciary. Next, the Consumer Protection Rule is explained and its application to Merrill Lynch's misuse of customer funds, where the company did not deposit customer cash in a reserve account, thereby putting customer money at risk in the event of bankruptcy. The five Anti-Money Laundering pillars are listed, including designating a compliance officer, completing risk assessments, building internal controls and AML policies, monitoring and auditing an AML program, and performing customer due diligence. Third, the Stanley Smith Barney, LLC and the UBS Group AG subsidiaries UBS Financial Services, Inc. and UBS Securities, LLC anti-money laundering cases are evaluated.

Fourth, a fictitious scenario illustrates the consequences that may occur when a registered representative for a broker/dealer uses their personal email to communicate with customers about business-related matters, including potentially violating Financial Industry Regulatory Authority rules. Fifth, three financial compliance surveillance cases are highlighted, demonstrating that financial compliance can be breached inadvertently or because of the seeming incompetence of a Chief Compliance Officer. Sixth, a fictitious scenario is portrayed, where a fake retail account is discovered and what should be done to rectify the situation.

Seventh, the Société Générale scandal is outlined, and whether Jérôme Kerviel was a culprit who was formatted and distorted by the company. The facts indicate that both issues were involved in the scandal. Eighth, a fictitious scenario is provided, where an individual with 30 years of experience working for a broker/dealer decides to become an investment adviser. The section explores the advantages and disadvantages of hiring such an individual. Finally, a fictitious scenario is given in which three possible unauthorized trades occur. The article explores the conditions under which the trades were genuinely unauthorized.

These cases and scenarios remind us that things should be taken at a different level than face value. A certain amount of disbelief is essential to certify fairness and justice. Retail financial compliance cases and scenarios usually contain many shades of gray, where doubt can be effectively employed to expose material facts. Only then can an accurate picture of a situation be evaluated.

KEYWORDS: Anti-Money Laundering, Consumer Protection Rule, Email Misuse, Fake Retail Accounts, Financial Compliance Definitions, Hiring an Investment Adviser, Ignoring Financial Compliance Rules, Technological Compliance, Unauthorized Trades,

INTRODUCTION

This article is divided into nine major sections. The first section specifies financial compliance definitions, including a fiduciary, a fiduciary's standard of care, and a broker/dealer. It then discusses whether a broker/dealer is a fiduciary and the relationship between the Securities Exchange Commission (SEC) and the fiduciary standard of care. The second section talks about the Consumer Protection Rule (CPR) and its application to Merrill Lynch's misuse of customer funds, where the company did not deposit customer cash in a reserve account, thereby putting customer money at risk in the event of bankruptcy. The third section concerns the five Anti-Money Laundering (AML) pillars, including designating a compliance officer, completing risk assessments, building internal controls and AML policies, monitoring and auditing an AML program, and performing customer due diligence (CDD). The third section reviews Morgan Stanley Smith Barney, LLC (MSSB) and the UBS Group AG (UBS) subsidiaries UBS Financial Services, Inc. (UBSFS) and UBS Securities, LLC (UBSS) AML cases.

The fourth section is a fictitious scenario in which a registered representative for a broker/dealer uses their personal email to communicate with customers about business-related matters. The scenario explores under what circumstances the registered representative violated Financial Industry Regulatory Authority (FINRA) rules. The fifth section discusses three financial compliance surveillance cases, demonstrating that financial compliance can be breached inadvertently or because of the seeming incompetence of the Chief Compliance Officer (CCO). The sixth section is a fictitious scenario in which a fake retail account is discovered and what should be done to rectify the situation.

The seventh section examines the Société Générale (SocGen) scandal and whether Jérôme Kerviel was the sole culprit or whether he was formatted and distorted by SocGen. The facts indicate that both issues were involved in the scandal. The eighth section is a fictitious scenario where an individual with 30 years of experience working for a broker/dealer decides to become an investment adviser. The section explores the advantages and disadvantages of hiring such an individual. The final section is a fictitious scenario in which three possible unauthorized trades occur. The questions raised in this section delve into the conditions under which a trade is genuinely unauthorized.

The cases and scenarios presented herein remind us that things should not automatically be taken at face value. A certain amount of skepticism is needed to ensure fairness and justice. Retail financial compliance cases and scenarios are fraught with nuances and ought to be viewed with some doubt and cynicism until most or all of the material facts have been exposed to the light of day. Only then can an accurate picture of a situation be evaluated.

FINANCIAL COMPLIANCE DEFINITIONS

This section aims to discuss whether it is appropriate to apply the fiduciary standard of care to broker/dealers. The first section following this introduction defines a fiduciary. The next section defines the fiduciary standard of care, observing that it is a strict standard of care in contrast to the suitability standard, which is more relaxed. The third section defines the notion of a broker/dealer. The fourth section specifies under what conditions a broker/dealer is a fiduciary. The fifth section argues that the SEC should not always deem a broker/dealer a fiduciary. The section concludes by observing that an investor is responsible for determining whether a broker/dealer or one of its representatives is acting in a fiduciary capacity.

Definition of a Fiduciary

According to Hayes, a fiduciary is an individual or an organization that "act[s] on behalf of others and are required to put the client's interests ahead of their own, with a duty to preserve good faith and trust."[1] This means fiduciaries are legally and ethically obligated to act in the principal's or client's interests.[2] The Consumer Financial Protection Bureau (CFPB) defines a fiduciary as someone who "manages money or property for someone else."[3] A person named a fiduciary must legally manage another's property or money for their benefit.[4] According to Black's Law Dictionary, a fiduciary is a person who "is required to act for the benefit of another person on all matters within the scope of their relationship; one who owes to another the duties of good faith, trust, confidence, and candor."[5] An officer of a corporation is an example of a fiduciary.[6]

Definition of the Fiduciary Standard of Care

The fiduciary standard was established by the Investment Advisors Act (IAA) of 1940, a federal law passed to monitor and regulate the actions of investment advisers.[7] The IAA is regulated by the SEC. The standard states that fiduciaries must prioritize the interests of their principal or client over their own, regardless of the effect on the fiduciary or their income.[8] The four essential duties that comprise the fiduciary of care include:[9]

- **Act only in the best interest of the principal or client** – A fiduciary is dealing with someone else's money or property, and the decisions made by a fiduciary should be the best decision for the principal or client and not necessarily for the fiduciary.
- **Manage money and property of a principal or client carefully** -A fiduciary has important financial responsibilities that must be carried out carefully. A fiduciary may be required to pay bills, oversee bank accounts, and pay for things the principal or client needs. A fiduciary may also be responsible for investments, paying taxes, collecting rent or unpaid debts, or obtaining insurance for a principal or client.
- **Keep the money and property of a principal or client separate from the fiduciary's money or property**—A fiduciary should never mix their money or property with the money or property of a principal or client. Documents that record such a mixture can violate the law.

---

[1] Adam Hayes, Fiduciary Definition: Examples and Why They Are Important, *Investopedia* (Mar. 19, 2024), *available at* https://www.investopedia.com/terms/f/fiduciary.asp.
[2] *Id.*
[3] CFPB Staff, What Is a Fiduciary, *Consumer Financial Protection Bureau* (Jun. 27, 2023), *available at* https://www.consumerfinance.gov/ask-cfpb/what-is-a-fiduciary-en-1769/#:~:text=A%20fiduciary%20is%20someone%20who,for%20their%20benefit%2C%20not%20yours.
[4] *Id.*
[5] BRYAN A. GARDNER (ED. IN CHIEF), BLACK'S LAW DICTIONARY 658 (West Publishing Co. 8th ed. 1999).
[6] *Id.*
[7] 15 U.S.C. § 80b-1 through 15 U.S.C. § 80b-21.
[8] Beacon Pointe Staff, Does Your Advisor Use The Right Standard? Fiduciary vs. Suitability, *Beacon Pointe* (n.d.), *available at* https://beaconpointe.com/does-your-advisor-use-the-right-standard-fiduciary-vs-suitability/#:~:text=Established%20as%20part%20of%20the,them%20personally%20or%20their%20income.
[9] CFPB Staff, *supra*, note 2.

- **Keep good records** – A fiduciary must keep that are true, correct, and complete records of the money or property of a principal or client, or face serious legal consequences.

The fiduciary standard is related to the prudent person rule.[10] Here, a fiduciary may only invest in securities that a reasonable person would purchase, where such purchases are evaluated from the perspectives of probable income and safety.[11]

In contrast to the fiduciary standard, the suitability standard states that fiduciaries "simply have to give advice that is suitable for a client based on their financial needs, objectives, and specific circumstances."[12] In other words, under the suitability standard, a fiduciary is not required to provide the best advice as long as the advice given is not bad. For example, under the suitability rule, a fiduciary can recommend investments that pay high commissions if the investment is consistent with a principal's or client's overall goals, even though better investments are available, such as no-load mutual funds.[13]

Definition of a Broker/Dealer

According to the SEC, a broker/dealer is "any person engaged in buying or selling securities for the account of others."[14] In other words, a broker/dealer is any individual or organization whose business is the buying and selling securities, but not necessarily for their own account.[15] According to Hayes, a broker/dealer is a "person or firm in the business of buying and selling securities for its own account or on behalf of its customers."[16] The term broker/dealer describes a stock brokerage house because these companies can act as agents and principals. A broker/dealer acts as a broker when it buys and sells securities on behalf of its clients, whereas it acts as a dealer when it buys and sells securities for its account.[17] According to Black's Law Dictionary, a broker/dealer is a "brokerage firm that engages in the business of trading securities for its own account (i.e., as a principal) before selling them to customers."[18] A broker/dealer is usually registered with the SEC and in the states where it does business.[19]

Is a Broker/Dealer a Fiduciary?

There is a significant difference between a fiduciary and a broker/dealer. A fiduciary cannot legally act in its interest but must act in the principal's or client's best interest.[20] If a fiduciary has a conflict of interest with a principal or client, they are legally required to raise the issue, whereas a broker/dealer acts out of inherent self-interest.[21] For example, many investment brokers sell products from their accounts. If the firm does not benefit from an individual buying a given product, the broker/dealer will likely not sell it, even if the sale is in the client's best interest.[22]

The critical issue is whether a broker/dealer is a fiduciary. Currently, the only time a broker/dealer is a fiduciary is when the broker/dealer is dually licensed as a broker/dealer and a registered investment adviser.[23] However, this statement has a caveat. According to Goldie and Murray, people should be aware of the "hat-changing" issue.[24] This issue occurs when a person receives investment advice or a sales pitch. When a broker/dealer or a representative provides investment advice, they act as a fiduciary, whereas if they give a sales pitch, they are not a fiduciary. The problem facing many investors is: When are the words from a broker/dealer or its representatives' investment advice or a sales pitch?

Uncertainty may be laid to rest in a broker/dealer's response to the following three questions:[25]

- Is the person a broker/dealer?
- Is the person a registered representative?

---

[10] James Chen, Prudent-Person Rule: What It Is, How It Works, *Investopedia* (Apr. 28, 2022), *available at* https://www.investopedia.com/terms/p/prudentmanrule.asp.
[11] *Harvard College v. Amory*, 26 Mass. 446 (1830), *available at* https://www.law.cornell.edu/wex/harvard_college_massachusetts_general_hospital_v._armory_(1830).
[12] Beacon Point Staff, *supra*, note 8.
[13] *Id.*
[14] SEC Staff, What Is a Broker/Dealer?, *U.S. Securities and Exchange Commission: Office of the Advocate for Small Business Capital Formation* (n.d.), *available at* https://www.sec.gov/files/oasb-broker/dealer-building-block.pdf.
[15] *Id.*
[16] Adam Hayes, What Is a Broker/dealer (B-D), and How Does It Work?, *Investopedia* (Mar. 3, 2024), *available at* https://www.investopedia.com/terms/b/broker/dealer.asp.
[17] *Id.*
[18] Bryan A. Gardner (ed. in chief), *supra*, note 8 at 205.
[19] *Id.*
[20] Curio Staff, Broker Vs. Fiduciary: How Are They Different?, *Curio Wealth* (Jul. 18, 2022), *available at* https://curiowealth.com/broker-vs-fiduciary-how-are-they-different/#.
[21] *Id.*
[22] *Id.*
[23] Nicholas Economos, 5 Huge Differences Between a Fiduciary and a Broker (Part 1), *Fiduciary Financial Partners* (Apr. 11, 2022), *available at* https://www.fiduciaryfinancialpartners.com/blog/5-huge-differences-between-a-fiduciary-and-a-broker-part-1.
[24] DANIEL C. GOLDIE, & GORDON S. MURRAY, THE INVESTMENT ANSWER (Dan Goldie Investment Services 2010).
[25] Nicholas Economos, *supra*, note 23.

- Does the person have a Series 6 or 7 license?

No matter what kind of license a person may possess, a Series 65 license must be the decisive criterion of a person's fiduciary duty.[26] Suppose investors want to be sure that the person they are working with is a fiduciary and that no conflict of interest exists. In that case, they should work with an investment adviser and pay their fee rather than ask for advice from a broker/dealer.

However, when obtaining financial information from a broker/dealer, a person should ask the broker/dealer whether the information provided is investment advice or a sales pitch. If the broker/dealer states that the information is investment advice, one can likely conclude that the broker/dealer is acting in a fiduciary capacity. However, suppose the response from the broker/dealer indicates that the information is a sales pitch or no response is provided. In that case, the probable conclusion is that the broker/dealer is not acting as a fiduciary. The difference is huge, but the responsibility of asking these questions is with the investor.

The Securities and Exchange Commission and the Fiduciary Standard of Care

The problem with the SEC requiring that a broker/dealer adhere to the fiduciary standard is that the broker/dealer is a profit-making enterprise. First and foremost, the courts have determined that the purpose of a corporation is to maximize shareholder value.[27] If a broker/dealer were to be considered a fiduciary, it would likely have to charge fees for the advice given. This may not be in the best interest of its customers. Also, the fee schedule could be unwieldy. The representatives of a broker/dealer may not be intimately aware of a client's financial situation, and a client may not be willing to reveal their financial situation to a broker/dealer. For these reasons, it is probably not advisable for the SEC to hold a broker/dealer to the fiduciary standard. Instead, the suitability standard is likely more realistic for the SEC.

Financial Compliance Definitions Conclusion

Thus, whether the fiduciary standard of care applies depends on the status of the broker/dealer (i.e., whether the broker/dealer holds a Series 65 license) or whether the broker/dealer is giving investment advice or advocating a sales pitch. The former is easy to determine because an investor needs to ask a broker/dealer whether they hold a Series 65 license. The latter is fraught with error because the answer depends on the words conveyed to an investor. Caveat emptor is the order of the day.

CONSUMER PROTECTION RULE AND MERRILL LYNCH

This section discusses the CPR and its application to Merrill Lynch's financial shenanigans during and after the 2008-09 financial crisis. It describes the issues surrounding Merrill Lynch's violations of the CPR. The firm comingled customer securities and monies with the securities and monies in its clearance account, thereby exposing innocent customers to potential bankruptcy obligations had the firm failed due to the disaster. Merrill Lynch was fined $415 million, even though the firm fully cooperated with the SEC in uncovering its past misdeeds.

Customer Protection Rule

The CPR is part of the SEC Rule 15c3-3, which "applies to a broker or dealer registered under section 15(b) of the Act (15 U.S.C. 78o(b)), including a broker or dealer also registered as a security-based swap dealer or major security-based swap participant under section 15F(b) of the Act (15 U.S.C. 78o-10(b))."[28] Essentially, the CPR requires a broker/dealer to protect customer assets by segregating them from the firm's assets.[29]

The CPR was established in 1972 as Congress reacted to the Paperwork Crisis on Wall Street from 1967 to 1970.[30] Before the widespread proliferation of computers, traders on the New York Stock Exchange (NYSE) and other trading exchanges employed paper slips from messengers to complete trades.[31] As the volume of trades expanded to 13 million trades per day, many small broker/dealers could not complete trades.[32] Many securities were lost or stolen. Organized crime rings purloined about $400 million in securities during the crisis, where many firms went bankrupt as customers experienced significant losses.[33] The idea behind SEC Rule 15c3-3 was to reduce the criminal effect of the crisis and prevent another crisis from occurring. With computer trading

[26] *Id.*
[27] *Dodge v. Ford Motor Co.*, 204 Mich 459; 170 NW 668 (1919), *available at* https://casetext.com/case/dodge-v-ford-motor-co.
[28] FINRA Staff, SEA Rule 15c3-3 and Related Interpretations, *Financial Industry Regulatory Authority* (Feb. 23, 2023), *available at* https://www.finra.org/rules-guidance/guidance/interpretations-financial-operational-rules/sea-rule-15c3-3-and-related-interpretations.
[29] FINRA Staff, Segregation of Assets and Customer Protection: Regulatory Obligations and Related Considerations, *Financial Industry Regulatory Authority* (2024), *available at* https://www.finra.org/rules-guidance/guidance/reports/2023-finras-examination-and-risk-monitoring-program/segregation-assets-customer-protection#:~:text=and%20Related%20Considerations-,Regulatory%20Obligations,protect%20customer%20funds%20and%20securities.
[30] Mark Hendricks, A Guide to SEC Rule 15c3-3, *Smart Asset* (May 30, 2023), *available at* https://smartasset.com/investing/sec-rule-15c33.
[31] *Id.*
[32] *Id.*
[33] *Id.*

becoming increasingly pervasive, where billions of shares are traded daily, SEC Rule 15c3-3 ensures that trades are predominantly secure from criminal activity.[34]

Merrill Lynch and the Customer Protection Rule

On June 23, 2016, the SEC announced that Merrill Lynch had agreed to pay a $415 million fine ($57 million in disgorgement and interest and a $358 million penalty) by admitting that it had misused customer funds to create profits for the company by failing to protect customer securities from claims from the firm's creditors.[35] Essentially, Merrill Lynch did not deposit customer cash in a reserve account. The company was involved in complex options trades that artificially decreased the monies deposited in customer reserve accounts. From 2009 to 2012, the action released billions of dollars per week so that Merrill Lynch could finance its own trading endeavors.[36] The issue was that had the firm gone bankrupt, customers would have seen a huge reduction in their reserve accounts.

Furthermore, Merrill Lynch violated the CPR by not holding customer securities in lien-free accounts that would have shielded the accounts from the firm's creditors. From 2009 to 2015, the company held at most $58 billion per day of customer securities in a clearing account.[37] This money was subject to third-party liens. Had Merrill Lynch failed, customers would likely have been able to recover their securities. According to Andrew J. Ceresney, the former director of the SEC's Division of Enforcement, the firm violated the CPR during the 2008 financial crisis, when the risk of failure was at its highest in recent memory.[38]

Along with the case against Merrill Lynch, the SEC published a two-part initiative to help reveal other abuses of the CPR. In the first prong, broker/dealers were required to proactively report possible violations of the CPR so that the firms could obtain cooperation credit and favorable settlement terms in an enforcement recommendation stemming from self-reporting.[39] In the second prong, the SEC Enforcement Division, the Division of Trading and Markets (DTM) and the Office of Compliance Inspections and Examinations (OCIE), decided to conduct risk-based examinations of specific broker/dealers to determine whether they complied with the CPR.[40]

Additionally, Merrill Lynch violated the Exchange Act Rule 21F-17 by employing language in its employee severance agreements that hindered employees from revealing illegal activities to the SEC.[41] As part of the settlement with the SEC, the company agreed to revise its employee agreements, policies, and procedures, including instituting a mandatory whistleblowing training program for all employees, including the employees of its parent corporation, Bank of America. Merrill Lynch and Bank of America consented to annually give their employees a summary of their rights and protections under the SEC's Whistleblower Program.[42]

Finally, the SEC order found that Merrill Lynch violated Securities Exchange Act Sections 15(c)(3) and 17(a)(1) and Rules 15c3-3, 17a-3(a)(10), 17a-5(a), 17a-5(d)(2)(ii), 17a-5(d)(3), 17a-11(e), and 21F-17.[43] The firm's subsidiary, Merrill Lynch Professional Clearing Corporation, was accused of violating Sections 15(c)(3) and 17(a)(1) and Rules 15c3-3, 17a-3(a)(10) and 17a-5(a). For the record, Merrill Lynch fully collaborated with the SEC by engaging in a far-reaching remediation process, including hiring an independent consultant to evaluate its CPR compliance.[44]

Consumer Protection Rule Conclusion

In conclusion, Merrill Lynch was caught by the SEC mixing customer securities and monies with its securities and monies. This illegal action could have resulted in significant customer losses had the company failed. During the 2008-09 financial crisis, there was a non-trivial probability that the firm would fall into bankruptcy when, on September 5, 2008, Goldman Sachs downgraded Merrill Lynch's stock to "conviction sell."[45] Bloomberg News reported that the company had lost $51.8 billion in 2008 dollars on mortgage-backed securities during the 2008 subprime mortgage crisis.[46] In other words, had Merrill Lynch not agreed to be purchased by Bank of America on September 14, 2008, at the apex of the financial crisis, the company would have most likely

[34] *Id.*
[35] SEC Staff, Merrill Lynch to Pay $415 Million for Misusing Customer Cash and Putting Customer Securities at Risk, *U.S. Securities and Exchange Commission* (Jun. 23, 2016), *available at* https://www.sec.gov/news/press-release/2016-128.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] Infinite, Merrill Lynch Cut to 'Sell' at Goldman on Writedowns, *Bloomberg News* (Sep. 5, 2008), *available at* https://infiniteunknown.net/2008/09/06/merrill-lynch-cut-to-sell-at-goldman-on-writedowns/.
[46] *Id.*

failed, and Merrill Lynch customers would have been liable for the broker/dealer's debts during its bankruptcy. Thus, the threat of failure was quite real, and the SEC's response was judiciously reasonable and appropriate.

ANTI-MONEY LAUNDERING, MORGAN STANLEY, AND THE UBS GROUP

This section compares and contrasts the behavior of Morgan Stanley Smith Barney, LLC and the UBS Group AG subsidiaries UBS Financial Services, Inc. and UBS Securities, LLC. The five anti-money laundering pillars are highlighted in the section following this introduction. The third section briefly analyzes the MSSB violations, listing the violated federal regulations. In the fourth section, the UBS anti-money laundering breaches are discussed. The fifth section compares and contrasts the violations of the two acceptance, waiver, and consent (AWC) documents. The final section concludes that one difference between the behavior of Morgan Stanley and UBS is that UBS violated both the FINRA and the National Association of Securities Dealers (NASD) regulations, whereas MSSB only violated FINRA regulations. Two other differences include the volume of transactions and their associated amounts, plus the value of the fines.

Five Anti-Money Laundering Pillars

According to Stankevičiūtė, the five AML pillars are:[47]

- Designating a compliance officer;
- Completing risk assessments;
- Building internal controls and AML policies;
- Monitoring and auditing an AML program; and
- Performing customer due diligence.

Designating a Compliance Officer

A company must employ an individual responsible for the firm's AML program. This person's duties include ensuring compliance, sharing their AML expertise with the rest of the company, assessing current processes and creating new ones, and aligning the entity's strategies with all current AML regulations that have been effectively implemented.[48] When designating a compliance officer, they should stay current with AML regulations, recommend compliance modifications predicated on audit findings, train and update employees regarding any changes in compliance regulations, and convey these changes to management and stakeholders.[49]

Completing Risk Assessments

To ensure a vigorous AML compliance program, a company must generate unblemished protocols, controls, and procedures for identifying financial crime based on the level of risk. From a practical perspective, the protocols, controls, and procedures should verify a customer's identity and report suspicious activities to senior management and the appropriate authorities.[50] It should be remembered that risk assessments are dynamic, not static. Risk assessments need to be periodically reviewed and updated to adjust to institutional changes in operation, regulatory revisions, and evolving risks.[51] Customers should be categorized based on their risk level. High-risk customers (e.g., politically exposed persons (PEPs)) or individuals from high-risk jurisdictions may necessitate a higher level of scrutiny or enhanced due diligence (EDD). Finally, transactions should be monitored in real-time to identify specific suspicious transactions.

Building Internal Controls and Anti-Money Laundering Policies

Establishing a well-defined compliance program is important for effectively managing corporate risks. In other words, a compliance department must stay informed about emerging market trends and new compliance regulations. For example, many organizations adopt environmental, social, and governance (ESG) policies that meet customer expectations.[52] Every member of the compliance team should receive training on how compliance impacts their job and on the tools and applications for detecting and reporting fraud. Although third-party organizations offer compliance training programs, training is not a one-time event but should be done periodically to ensure that individuals are aware of regulation updates.[53]

---

[47] Gabija Stankevičiūtė, What are the Five Pillars of AML Compliance?, *iDenfy* (Sep. 15, 2023), *available at* https://www.idenfy.com/blog/five-pillars-of-aml-compliance/.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*

Nine Cases and Scenarios Involving Retail Financial Compliance

Monitoring and Auditing Your Anti-Money Laundering Program

Compliance programs must be regularly audited by independent third parties. Such audits help recognize potential vulnerabilities and uphold operational integrity. Compliance program audits are distinct from financial audits because they focus on AML regulations to safeguard against criminal activity.[54] A compliance audit should be performed at least once yearly, preferably semi-annually or quarterly. An independent compliance audit is critical in identifying weaknesses, improving practices, and revealing compliance to regulatory bodies.[55]

Performing Customer Due Diligence

In May 2018, the Financial Crimes Enforcement Network (FinCEN) instituted the CDD rule. The rule requires firms to ascertain and verify their customers' identities and continuously detect, monitor, and report suspicious customer activities. The four CDD elements include:[56]

- Verify the identity and assess the risk level of every customer;
- Determine the beneficial owners of legal entities;
- Understand and appreciate the nature of customer relationships; and
- Continuously monitor transactions, looking for suspicious behaviors or patterns.

The CCD rule posits a risk-based approach where entities evaluate customers and transaction requests based on the level of risk. A firm can customize its due diligence efforts by assessing risks affiliated with customers and transactions. When addressing higher-risk situations, such as a customer from an area where money laundering is common, a company should apply enhanced due diligence (EDD) measures.[57]

Morgan Stanley Smith Barney, LLC Anti-Money Laundering Case

The SEC suit was against MSSB.[58] When listing the charges below, the prefix used is "MS-nn," when "nn" is the number of the charge. The charges against Morgan Stanley by the Department of Enforcement of FINRA are as follows:

- MS-01: MSSB did not conduct reasonable wire and foreign currency transfer surveillance.
- MS-02: MSSB failed to investigate suspicious wire transfers reasonably.
- MS03: MSSB did not reasonably inspect penny stock trading for AML issues;

For MS-01, from January 2011 until at least April 2016, some of the MSSB wire processing systems suffered significant design limitations and programming flaws, which resulted in tens of billions of dollars of wire and foreign currency transfers not being examined, including to and from jurisdictions possessing a high money laundering risk, thereby violating FINRA Rules 3310(a) and 2010.[59] For MS-02, from January 2011 to December 2013, MSSB did not allocate sufficient resources to evaluate alerts created by its automated AML system. The firm's analysts frequently closed alerts without sufficiently conducting or documenting their investigations of suspicious wire transfers, thereby violating FINRA Rules 3310(a) and 2010.[60] Finally, for MS-03, from January 2011 to December 2013, MSSB's AML Department neglected to reasonably oversee the deposits and trades of low-priced securities or penny stocks by customers for potential AML issues, including insider trading and market manipulations, thereby violating FINRA Rules 3310(a) and 2010.[61]

UBS Group AG Anti-Money Laundering Case

The suit against UBS was divided into two parts: charges against UBSFS and UBSS, both of which are subsidiaries of UBS.[62] When listing the charges below, the prefix used is "UBS-nn," when "nn" is the number of the charge. The charges against UBSFS and UBSS by FINRA are as follows:

- UBS-01: UBSFS did not possess an AML program that was reasonably designed to inspect foreign currency wire transfers for possible suspicious activity.
- UBS-02: UBSS did not retain an AML program that was reasonably programmed to scrutinize penny stock transactions for possible suspicious activity.

---

[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] FINRA Staff, Letter of Acceptance, Waiver, and Consent, No. 2014041196601, *Financial Industry Regulatory Authority* (Dec. 12, 2018), *available at* https://www.finra.org/sites/default/files/Morgan_Stanley_AWC_122618.pdf.
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] FINRA Staff, Letter of Acceptance, Waiver, and Consent, No. 2012034427001, *Financial Industry Regulatory Authority* (Dec. 17, 2018), *available at* https://www.finra.org/sites/default/files/UBS_AWC_121718.pdf.

- UBS-03: UBSFS and UBSS did not establish a due diligence program that was reasonably designed for correspondent accounts.

For UBS-01, from January 2004 to April 2017, UBSFS violated NASD Rule 3310(a) and FINRA Rule 3310(a) when it did not have an AML program reasonably designed to detect and report suspicious foreign currency wire transfers.[63] For UBS-02, from January 2013 to June 2017, UBSS violated FINRA Rule 3310(a) when it did not possess a reasonably designed AML program to detect and report suspicious activity regarding low-priced equity securities or penny stock transactions via an omnibus account.[64] Finally, for UBS-03, from May 2011 to August 2012 and from May 2008 to September 2017, respectively, UBSFS and UBSS violated NASD Rule 3011(b) and FINRA Rule 3310(b) when the companies did not employ risk-based procedures and controls to every correspondent account of Foreign Financial Institutions (FFIs) that were reasonably devised to detect and report possible money laundering activities. The companies did not conduct periodic reviews of the correspondent account activities of FFIs to determine the consistency of information regarding the type, purpose, and anticipated activity of an account, as demanded by 31 C.F.R. § 1010.610(a). In other words, UBSFS violated FINRA Rules 3310(b) and 2010, and UBSS violated NASD Rules 3011(b) and 2110 and FINRA Rules 3310(b) and 2010.

Comparison of the Two Cases

This section is divided into three subsections. The first subsection compares and contrasts which AML pillars MSSB and UBS violated. The second subsection discusses the number of wire transfers and amounts of money transferred without being monitored. The third and final subsection evaluates the fines imposed on MSSB and UBS by FINRA.

Comparison of Anti-Money Laundering Pillars Violated

The comparison of UBS and Morgan Stanley cases will be conducted by examining the cases in terms of the five AML pillars. A table will be constructed where the first column contains the five AML pillars. The second column will indicate which of the five pillars Morgan Stanley violated, whereas the third column will show which one of the five pillars UBS breached. If a row in column one has Morgan Stanley and UBS entries, then there is a basis for comparing the organizations for that principle. If there is an entry in the second column but not in the third column, then Morgan Stanley violated a principle not broken by UBS. On the other hand, if there is an entry in the third column but not in the second column, then UBS violated a principle that was not broken by MSSB. For a given principle, if there are no entries for columns two and three, then the breaking of that pillar was not present in either of the two cases. Here is the table in question:

Anit-Money Laundering Pillars	Morgan Stanley Case	UBS Case
Designating a compliance officer	Not applicable	Not applicable
Completing risk assessments	MS-01, MS-02	UBS-01, UBS-02
Building internal controls and anti-money laundering policies	MS-01, MS-02	UBS-01, UBS-02
Monitoring and auditing an anti-money laundering program	MS-01, MS-03	UBS-01, UBS-02
Performing customer due diligence	MS-01, MS-02, MS-03	UBS-01, UBS-02, UBS-03

The first thing to notice is that it can be assumed that both MSSB and UBS had designated a compliance officer because lacking a compliance officer was not part of the two AWC letters. Second, both organizations had issues in completing risk assessments, if only because their risk assessment protocols, control, and procedures were less than reasonable due to the inability of their automated AML systems to capture wire and foreign currency transactions, particularly from jurisdictions where money laundering was common. Third, the building of internal controls and AML policies was insufficient because the companies typically relied on automated AML software to catch suspicious activity rather than supplementing the automated results with manual intervention. Fourth, there was a failure to scrutinize both entities' low-priced or penny stock transactions, probably due to the opinion that fraud is likely negligible for these kinds of dealings. Finally, MSSB and the UBS subsidiaries failed to conduct vigorous customer due diligence.

It is interesting to note that FINRA charged MSSB with violations of rules 3310(a) and 2010, whereas the federal agency accused UBS of violating NASD Rules 3310(a), 3011(b), and 2110 and FINRA Rules 3310(a), 3310(b), and 2010. The fact that UBS violated NASD rules and FINRA rules while MSSB only violated FINRA rules is interesting. Because UBS violated NASD and FINRA rules, this fact seemingly indicates that UBS's behavior may have been more egregious than MSSB's.

[63] *Id.*
[64] *Id.*

Neither firm had any formal disciplinary history when the two AML letters were made public.[65] [66] MSSB had been a FINRA member since 2009, while the UBS subsidiaries were FINRA members, UBSFS and UBSS, but the AML did not state the year they joined the organization. MSSB's egregious behavior began in 2011,[67] while UBS's conduct started in 2004,[68] indicating that UBS had seven additional years to rectify its anti-money laundering policies, controls, and procedures compared to MSSB.

Wire Transfer Numbers and Amounts

Regarding the number of wire transfers not surveilled, MSSB failed to inspect through the Transaction Monitoring System (TMS) 140,000 transactions totaling $43 billion of wire transfers via Global Currence and FX Ion systems for five years.[69] From December 2014 to April 2016, MSSB did not surveil 267 incoming wires, which amounted to $30.4 billion.[70] From January 2014 to August 2015, the company failed to send TMS data on 91,00 outgoing transactions amounting to $25.5 billion. As for the penny stock issue, MSSB did not detect nor report the movement of 2.7 billion shares amounting to $164 million.[71]

In contrast, from 2009 to 2012, UBSFS sent or received over 199,000 foreign currency wires at $9.7 billion.[72] Of these transfers, 17,500 for $464 million were from high-risk countries, such as Mexico, Turkey, Thailand, Argentina, and Saudi Arabia.[73] Also, from 2009 to 2012, in terms of customer commodity accounts, UBSFS experienced $6.2 billion in currency wires, of which $350 million came from high-risk jurisdictions.[74] About 178,700 foreign currency wires totaling $3.7 billion from 2009 to 2012 were not surveilled for retail brokerage accounts. From January 2012 to June 2017, UBSS enabled the sale of 30 billion shares of penny stock valued at $545 million without collecting essential information, such as the stock's beneficial owner, the beneficial owner's relationship to the stock issuer, or how the customer came to own the stock.[75]

Penalties Paid by the Defendants

FINRA's penalties for MSSB and UBS are striking. FINRA censured MSSB and fined it $10 million. In contrast, UBSFS was censured and was required to pay a $4.5 million fine, while UBSS was also censured with a $500 thousand fine for a total of $5 million in fines. MSSB paid twice as many fines as UBS despite a seven-year discrepancy in the offending periods. Given the difference in the size of the fines, one could infer that the MSSB violations were more egregious than the violations enacted against UBS.

Anti-Money Laundering Conclusion

In conclusion, the table above indicates that the two companies' violations of the AML pillars were similar. Even so, the only difference between the two cases appears to be the size of the fines. The monetary difference in the fines may be caused by different factors, some of which may not have been specified in the AWC letters. This conclusion bears greater inspection.

SCENARIO OF EMAIL MISUSE

This section discusses the fictitious situation where Jason Poirot, a registered representative for a broker/dealer, used his personal email to communicate with customers about business-related matters. The piece first describes FINRA Rule 2210, which deals with correspondence, retail, and institutional communications. In the next section, the paper discusses the corrective and disciplinary actions that could be taken against Poirot. The section observes that it may be more poignant for the broker/dealer to use this situation as a teaching moment rather than employ draconian measures such as termination. The subsection concludes that FINRA Rule 2210 does not distinguish between new hires and seasoned veterans. Even so, a firm may decide to provide its registered representatives with corporate cell phones, which its employees may use for business and personal purposes, thereby assuring compliance with FINRA rules and regulations.

Financial Industry Regulatory Authority Rules that May Have Been Broken

The FINRA Rule 2210 deals with communications with the public.[76] The rule divides all communications into correspondence, retail, and institutional communications. It also establishes principles-based content standards that apply to communications

[65] FINRA Staff, *supra*, note 12.
[66] FINRA Staff, *supra*, note 16.
[67] FINRA Staff, *supra*, note 12.
[68] FINRA Staff, *supra*, note 16.
[69] FINRA Staff, *supra*, note 12.
[70] *Id.*
[71] *Id.*
[72] FINRA Staff, *supra*, note 16.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] FINRA Staff, Communications with the Public: Regulatory Obligations and Related Considerations, *Financial Industry Regulatory Authority* (2024*), available at* https://www.finra.org/rules-guidance/guidance/reports/2021-finras-examination-and-

technologies and practices under development. Rule 2210 includes standards for approval, review, and record-keeping procedures, and firms must release certain communications to FINRA.[77] According to the FINRA Staff, Rule 2201 demands that "all communications be based on principles of fair dealing and good faith, be fair and balanced, provide a sound basis for evaluating the facts "[regarding] any particular security or type of security, industry, or service' and include all 'material fact[s] or qualification[s]' necessary to ensure such communications are not misleading."[78] Rule 2210 also forbids false, misleading, promissory/exaggerated statements and projections regarding performance.[79]

FINRA requires registered firms to make and preserve records related to their business activities to monitor compliance.[80] Required records include emails between registered financial professionals and their customers. FINRA also demands that firms possess procedures for examining incoming and outgoing written and electronic communications such as emails and text messages.[81] However, FINRA and the SEC rules generally do not prohibit the employment of personal email accounts or text messaging applications. As "off-channel" communications, as long as a broker/dealer monitors, captures, and retains these records, no violation of FINRA Rule 2210 occurs.[82] Because this may be technologically difficult, many broker/dealers have internal policies that prohibit or seriously limit the use of personal communication channels.

Experience has demonstrated to FINRA that financial professionals who employ personal email or other off-channel vehicles are typically not compliant with their broker/dealer's policies and use personal email and text messaging to circumvent investor rules and regulations. According to FINRA, off-channel messages may include exaggerated claims regarding returns or performance or be employed to exert pressure on customers to decide quickly about an investment.[83] Finally, if a broker/dealer cannot monitor the communications of their financial professionals, the company cannot proactively identify issues that may impact customer investments.[84]

The issue is whether Poirot violated Rule 2210 when using his personal email to communicate with customers about business-related matters. The answer depends upon the ability of his broker/dealer to collect, monitor, and review his personal emails. If Poirot used his personal email account while at work where the email message employed corporate servers, he likely did not violate Rule 2210 provided that the broker/dealer could collect, monitor, and review his emails. This is not unreasonable because organizations typically collect, monitor, and review all emails that are sent through their servers.

On the other hand, if Poirot used his personal email account while he was not at work where the servers were not owned, leased, or operated by the broker/dealer, then Poirot likely violated Rule 2210 because his firm may not have been able to collect, monitor, and review the emails to his customers. Thus, a violation only exists if Poirot's broker/dealer was unable to collect, monitor, and review the financial professional's communications via his personal email account.

Corrective and Disciplinary Actions to Be Taken

The corrective action to be taken depends on several factors, one of them being the content of the emails sent to Poirot's customers. The question posits that Poirot is a registered representative, meaning that he passed the Series 6[85] examination and the Series 63[86] examination, also known as the Blue Sky Laws examination or the state security laws examination. Poirot may have also passed the Series 26[87] examination, making him a principal representative, but this is unlikely because the question specifically states that Poirot is a registered representative. It should be remembered that a registered representative position is an entry-level position at a broker/dealer. Poirot is likely not intimately aware of FINRA rules and regulations but only possesses sufficient understanding to pass the security examinations. Thus, initially, the more appropriate corrective action is probably to consider Poirot's understanding of securities laws. Additional training may be appropriate.

---

risk-monitoring-program/communications-with-public#:~:text=FINRA%20Rule%202210%20requires%2C%20among,"material%20fact%5Bs%5D%20or.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] FINRA Staff, Watch for These 5 Behaviors by Your Registered Financial Professional, *Financial Industry Regulatory Authority* (Sep. 19, 2023*), available at* https://www.finra.org/investors/insights/watch-these-5-behaviors-your-financial-professional#:~:text=Using%20Personal%20Email%20or%20Text%20Messages&text=Required%20records%20include%20communications%20between,communication%20like%20email%20and%20texts..

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] FINRA Staff, Series 6 – Investment Company and Variable Contracts Products Representative Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series6.

[86] FINRA Staff, Series 63 – Uniform Securities Agent State Law Exam, *Financial Industry Regulatory Authority* (2024), *available at* https://www.finra.org/registration-exams-ce/qualification-exams/series63.

[87] FINRA Staff, Series 26 – Investment Company and Variable Contracts Products Principal Exam, *Financial Industry Regulatory Authority* (2024), *available at* https://www.finra.org/registration-exams-ce/qualification-exams/series26.

If the content of the communication is personal in nature, such as an invitation to a party held by the customer, then there is likely no correction needed. Poirot may be personal friends with a customer, and the communication may have nothing to do with the broker/dealer. It should be remembered that personal friends are a financial professional's warm market, and communications among friends are not prohibited by Rule 2210. In this instance, as long as the communication is unrelated to the broker/dealer's business, no corrective action must be taken.

On the other hand, if the content of the email is business-related, then Rule 2210 comes into play. The broker/dealer must collect, monitor, and review Poirot's email to ensure compliance. The company can employ draconian measures and terminate the employee immediately, but this action is probably a waste of corporate funds because of the training costs of educating a financial professional. It would likely be more prudent to talk to Poirot and inform him that business-related emails should be sent using the firm's corporate email facility. The warning should be verbal; a written record may not be necessary, particularly if the email was innocently sent. It should be remembered that when employing severe measures, such action may have the unintended consequence of instilling fear within Poirot. The idea behind a discussion with Poirot is to educate him, not pit him against the broker/dealer.

One corrective action the firm could take is to provide Poirot and other financial professionals with a corporate cell phone and encourage them to communicate with their customers, personal friends, and acquaintances using this corporate device. In this way, they would not have to change devices when making personal communications. The advantage to the broker/dealer is that all communications would then be available for inspection by the firm, thereby adhering to Rule 2210.

Finally, if the use of personal emails is reoccurring, where Poirot is blatantly ignoring Rule 2210, then sterner action may be necessary. For example, if Poirot refuses to permit his broker/dealer to review his personal emails, termination may be necessary, and reporting him to FINRA and other federal securities agencies, such as the SEC and the NASD, may be appropriate. An issue that should likely not be considered in this instance is the volume of business that Poirot is bringing into the company. It is more important to be compliant because, in the long run, the negative consequences may overshadow the immediate short-run gain.

Email Misuse Conclusion

In conclusion, there may or may not be a violation of Rule 2210. It depends on the content of the emails and Poirot's behavior. Poirot may be a new hire, and disciplining him harshly may instill fear in him and other financial professionals, thereby creating an atmosphere of discontent with the company, to put it mildly. A better solution may be to look at the situation from a big-picture perspective and then determine what to do. FINRA Rule 2210 does not distinguish between new hires and seasoned veterans. Periodic training is essential in the financial services industry. Without the proper training, one cannot expect individuals to be omniscient. It is a narrow and strait path to walk, but necessary in a climate where regulations typically presume that a person is guilty until proven innocent.

THREE FINANCIAL COMPLIANCE SURVEILLANCE CASES

This section delves into the significant cases of In the Matter of Chardan Capital Markets, LLC (Chardan), In the Matter of Citigroup Global Markets, Inc. (CGMI), and In the Matter of Thomas E. Haider (Haider). These cases, which drew the attention of the SEC, are crucial as they highlight how the three firms violated securities laws, particularly by failing to identify offending behavior and not filing Suspicious Activity Reports (SARs) when required. This failure was typically caused by either malfeasance on the part of the CCO (e.g., Chardan and Haider) or a lack of a comprehensive automated computer system that failed to process compliance data correctly (e.g., CGMI). The latter usually happens when system analysts fail to comprehend the extent of an issue, even under the light of reasonable due diligence. Individuals are mere mortals, and they are not omniscient. The law is not necessarily forgiving regarding compliance. Nonetheless, justice must be served. It should be remembered that mercy cannot rob justice, for to do so, the world would be turned on its head.[88]

In the Matter of Chardan Capital Markets, LLC

In Chardan, the SEC found that from at least October 2013 to June 2014, Chardan failed to file a Suspicious Activity Report (SAR) when the company knew, suspected, or had reason to suspect that the firm was being used by customers to engage in either fraudulent activity or business activities without a legal purpose.[89] Chardan possessed compliance policies that specified red flags indicating suspicious activity. The SEC maintained that Chardan failed to conduct the necessary reviews of significant penny stock liquidations involving seven customer accounts during the abovementioned period. Chardan's clearing house, the Industrial and Commercial Bank of China Financial Services, LLC (ICBC), raised multiple concerns with Chardan regarding these seven customers and their trading in penny stocks. In June 2014, the ICBC halted clearing penny stock trades, and Chardan departed the penny stock business.

[88] King James Version, Galatians 6:7 and Book of Mormon, Alma 42:35.

[89] *In the Matter of Chardan Capital Markets, LLC*, Administrative Proceeding File No. 3-18486, *U.S. Securities and Exchange Commission* (May 16, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-83251.pdf.

Chardan never investigated these red flags or filed SAR reports during the relevant period. Thus, by not filing the SARs as demanded by law, Chardan willfully violated Section 17(a) of the Securities Exchange Act (SEA) of 1934 and Rule 17a-8.[90]
In late 2013, Chardan on-boarded seven new customers that regularly deposited and sold billions of shares of penny stocks. These customers usually attained these stocks by converting debentures into stock shares. At the time, Chardan had written AML policies and procedures that flagged possible money laundering and suspicious activity. The pertinent red flags included:[91]

- A customer or an individual affiliated with a customer has a questionable background or is listed in a news report regarding possible criminal activity;
- A customer desires to be involved in transactions that do not make business sense;
- A customer opens multiple accounts with the same beneficiary for no business purpose;
- Two or more accounts suddenly trade in illiquid stocks;
- Legal subpoena exists; and
- A customer wants to liquidate penny stocks, which results in an unregistered distribution.

Chardan-specific red flags were:[92]

- No business, no revenue, and no product;
- Frequent changes in the structure of a business;
- Company officer affiliated with penny stock issuers;
- Many changes in business strategy or line of business; and
- Customers that were previously involved in trading restrictions.

According to the SEC, additional Chardan red flags should have been:[93]

- An abrupt spike in investor demand with an increasing price of the relevant penny stocks;
- An electronic transfer to a customer with little or no assets under management; and
- The SEC filings for the penny stock are incomplete or do not exist.

The SEC opined that when these red flags were triggered, the then-Chardan CCO and AML Officer did not collect sufficient documentation to demonstrate how these seven customers obtained their shares of penny stocks. When the CCO and AML Officer did receive the requested documents from the customer, they barred the customer from trading but did not file a SAR report.[94] The SEC also observed that the CCO and AML Officer did not sufficiently examine customer trading patterns searching for suspicious activity. When the ICBC suspended trades for these seven customers, Chardan never investigated its customer trading activity or filed a SAR report, even though the firm knew of many of the above red flags.[95]

According to Sections 15(b) and 21C of the SEA, Chardan was ordered by the SEC to pay a fine of $1 million to the Commission, where the money was transferred to the general fund of the United States Treasury.[96] Essentially, this case exemplifies the legal consequences for broker-dealers who fail to respond sufficiently to red flags. The reasons why the firm did not adequately respond do not matter. What does matter is that either the response was insufficient or that a SAR report was not filed. The moral of the case is that compliance should be prioritized in a financial services company.

In the Matter of Citigroup Global Markets, Inc.

In CGMI, the SEC held that CGMI had committed a series of technological errors that had not been discovered for years, thereby violating federal securities laws that were related to trade surveillance, including its policies and procedures addressing principal transactions.[97] CGMI relied on automated trading systems to conduct its business. A failure to supervise this technology system led to a compliance failure and securities law violations. From 2002 to 2012, CGMI did not monitor thousands of trades that were executed by its trading desks. The failure happened because the reports employed by CGMI staff to review trades did not include thousands of trades. These electronic reports excluded relevant trades that should have been the subject of daily surveillance.[98]

From October 20007 through February 2010, the firm inadvertently directed more than 467,000 advisory client transactions to an affiliated market maker, Automated Trading Desk Financial Services LLC (ATD), which executed the transactions as a

[90] A willful violation of securities laws means "that a person charged with the duty knows what he is doing." *Wonsover v. SEC*, 205 F.3d 408(D.C. Cir. 2000), *available at* https://casetext.com/case/wonsover-v-securities-and-exchange-comm.
[91] *In the Matter of Chardan Capital Markets, LLC*, *supra*, note 2.
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *In the Matter of Citigroup Global Markets, Inc*., Administrative Proceeding File No. 3-16764, *U.S. Securities and Exchange Commission* (May 16, 2018), *available* https://www.sec.gov/litigation/admin/2015/34-75729.pdf.
[98] *Id.*

principal at or near prevailing market rates. It should be noted that CGMI attempted to prevent ATD from executing principal transactions by routing the transactions away from the firm. Furthermore, CGMI did not detect these principal transactions because it relied on an exception report that was not designed to capture any principal transactions executed via ATD.

The CGMI Information Barriers Surveillance Group (IBSG) is one of CGMI's Compliance departments. It controls and conducts trade surveillance procedures. The IBSG was responsible for overseeing daily trade surveillance to determine if CGMI personnel traded securities on the Loan Watch List (LWL) or the Restricted Trading List (RTL). The trade reports were populated by the data feed known as LoansQT, which contained only loan trades and did not contain loan desks' trades, swap trades, etc. These trades should have been prohibited by existing CGMI policies. This issue existed since 2002. As a result, for seven years, the IBSG did not inspect a percentage of the trading by a majority of loan desks.

The RTL surveillance experienced two problems. First, the loan desk trading reports did not comprise non-loan trades. Second, IBSG staff employed the "002" and "282" exception reports to check for firm-wide compliance. Unfortunately, both reports had legacy limitations. The 002 report included trades that were conducted by one of the two legacy platforms that the company inherited due to a series of corporate mergers.[99] The 282 report captured data from the two legacy platforms but was a position-based report that captured daily changes in positions, not position changes during the day, where, at the end of a day, a client's position remained unchanged. Essentially, the 282 report issue was a software coding error not identified until mid-2009. The issue was seemingly corrected in late 2009 but reappeared in 2012 during the SEC's investigation.[100]

Other issues in the CGMI systems needed to be fixed. First, the company's manual advisory account coding of all advisory orders was not necessarily recorded properly as a money-managed account (MMA). CGMI also failed to search for unauthorized principal transactions that resulted before the automation of MMA coding.[101] Had this research occurred, the obvious question would have been: What could CGMI do to rectify the situation? The horse was out of the barn, and trying to put it back in would not have changed anything.

Second, the database cross-referencing of advisory accounts ensured that if the account information on an order contained in the firm's order management system (OMS) matched the account information in the advisory account database, the order was designated "DNC," meaning "Do Not Cross." If there was no match, the software assumed that the order originated from a non-advisory brokerage account that could be sent to ATD.[102] The problem was that the advisory account database contained only some of the advisory accounts. In other words, for some reason, advisory accounts were not added to the advisory account database. From a computing perspective, unless were was an alternative mechanism, there was no way that the computer program could verify that an account not on the advisory account database was indeed an advisory account. Had the company created such a method, according to the SEC, it would have discovered that it had executed more than 100,000 principal transactions with ATD.[103]

CGMI should have tested whether its advisory account database was regularly updated by the new programming of its OMS. This oversight resulted in 467,000 principal transactions that were inadvertently sent to ATD.[104] The CGMI trade surveillance failed to identify these principal transactions for over two years because the firm relied on an inadequate exception report that was not designed to collect these transactions.

Based on the facts above, the issues discussed herein demonstrate the limitations of incorporating legacy systems of third parties into existing computer systems. Simply stated, one of the risks of merging companies for whatever good business reasons, the conglomeration of computer systems will likely be incomplete or inadequate merely because different entities process data differently. When integrating computer systems from diverse organizations, individuals usually attempt to analyze thoroughly the two systems. Even so, there is a risk of failing to detect all the issues, particularly when knowledgeable employees are laid off to increase the synergies of a merger. Second, and sometimes more importantly, when new systems are created, analysts may fail to recognize the nuances of an old system. This typically happens because individuals do not necessarily understand or appreciate the workings of a legacy system. There is no royal road here. Systems analysts are not omniscient, and mistakes and oversights will happen. There is no way around it. One should remember that hindsight is always 20/20.

In the Matter of Thomas E. Haider

In Haider, FinCEN opined that Thomas Haider willfully violated the Bank Secrecy Act (BSA) of 1970 and its associated regulations when he was the CCO and the Senior Vice President of Government Affairs at MoneyGram International, Inc. (MoneyGram) because he failed to implement and maintain an effective anti-money laundering program.[105] Since 2003, MoneyGram has been a

[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *In the Matter of Thomas E. Haider*, Number 2014-08, *U.S. Department of the Treasury: Financial Crimes Enforcement Network* (Dec. 18, 2014), *available at* https://www.fincen.gov/sites/default/files/shared/Haider_Assessment.pdf.

money transfer service that facilitated money transfers from one location to another across the globe. It consisted of independently owned organizations, such as convenience stores and Internet cafes, that were authorized to transfer money through its network. MoneyGram had to comply with the BSA and its affiliated regulations as a money transmitter. MoneyGram was obliged to implement and maintain an effective AML program as well as submit SARs to FinCEN that detected individuals and funds that were greater than $2,000.00 or were suspected of criminal activity. As CCO, Haider failed to:[106]

- Implement disciplinary policy regarding MoneyGram agents or outlets;
- Terminate known high-risk agents or outlets that posed an unreasonable risk of fraud and money laundering;
- File timely SAR reports on specific agents and outlets due to undue influence of the sales department on the agent and outlet disciplinary process;
- Implement policies to ensure that MoneyGram complied with the timely filing of SARs;
- Ensure that MoneyGram performed proper and effective audits of agents and outlets;
- Warrant that MoneyGram adequately screened new agents and outlets;
- Oversee adequate due diligence on agents and outlets.

MoneyGram consisted of the fraud, AML Compliance, risk, and sales departments. As CCO, Haider supervised AML Compliance and MoneyGram's Fraud department. He was responsible for ensuring that MoneyGram complied with the BSA and its associated regulations and day-to-day compliance efforts, particularly approving policy-related changes.[107] Thus, Haider was responsible for MoneyGram's failures to comply with the BSA and its affiliated regulations.

In particular, Haider did not terminate the 49 outlets with 25 or more Consumer Fraud Reports (CFR) from September 2006 to February 2007, even when the amount of money transferred was over $1,000.00, a potential fraud indicator. Four of the 49 outlets were Money Spot, Money Spot 2, Money Spot 5, and N&E Associates, all owned by James Ugoh.[108] Haider took no action even when the Toronto Police Department categorized Money Spot as "dirty" because it was found to have engaged in a practice known as "check pooling," where "checks were deposited into business accounts by individuals laundering the money."[109]

There were many examples of compliance issues in Haider. Haider did not ensure that the Fraud Department provided SAR analysts with the relevant data to file SAR reports, even after compliance consultants advised him of the necessity of the action. When MoneyGram performed audits of agents and outlets, their efforts were inadequate because the auditors were not trained to seek out the warning signs of fraud.[110] For example, an indication of possible fraud is when one MoneyGram outlet makes checks payable to another MoneyGram outlet. If audit visits did occur, they were informal rather than formal audits. In one instance, auditors were afraid to visit a particular outlet because they believed doing so would precipitate physical injury. Finally, Haider permitted new outlets to be opened even when the outlet was likely terminated by a competitor.[111]

This plethora of compliance failures resulted in Haider being assessed a $1 million civil penalty due to his willful violation of the BSA and its implementing regulations. Based on the information described above, Haider is likely an example of CCO incompetence. It is hard to reconcile Haider's actions and lack of action with competent CCO behavior. The frequency of Haider's inability to act in the presence of overwhelming evidence to terminate outlets leads one to consider that Haider was either grossly incompetent or illegally compensated by the offending outlets. There are seemingly no other reasonable explanations for his behavior. Although Haider does not delve into Haider's possible corruption, it seems to be the 800-pound gorilla in the room that no one acknowledges exists. Haider is an example of what not to do as a CCO. For these reasons alone, Haider is an important case to ponder, if only to show aspiring CCOs what behaviors to avoid.

Lessons Learned from These Three Cases

When addressing the lessons learned from these three cases, one must consider the policies, standards, controls, processes, and procedures in place at the different firms. Policies are at the top of a hierarchal triangle because they establish the expectations that direct a business.[112] Policies authenticate management intent and the corporate structure.[113] Standards and controls are in the middle of the triangle. Standards stipulate quantifiable requirements, whereas controls identify the conditions that the entity is expected to meet or satisfy, such as laws, regulations, and frameworks.[114] Processes and procedures are at the base of the triangle. They are the

[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] Alyssa Pugh, Policies vs. Standards vs. Controls vs. Procedures, *Tandem* (Jan. 5, 2023), *available at* https://tandem.app/blog/policies-vs-standards-vs-controls-vs-procedures.
[113] *Id.*
[114] CF Staff, Policies vs Standards vs Controls vs Procedures, *Compliance Forge* (n.d.), *available at* https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-

specific mechanisms an organization employs to satisfy the conditions expressed in the corporate controls, which in turn implement the business's policies.[115]

In Chardan, the SEC opined that when the various red flags were triggered, the CCO and AML Officer did not collect sufficient documentation on how the seven customers mentioned above obtained their penny stock shares.[116] The inability to gather the appropriate documentation indicates that the data collection procedure must be revised. Chardan also states that when the necessary data was collected, the CCO and AML Officer did not file a SAR report. This is likely a process or procedure failure because the relevant policy and control indicate that an SAR report should be generated when suspicious activity occurs. The SEC noticed that the CCO and AML Officer did not sufficiently examine the customer trading patterns, looking for suspicious activity. This is a control issue because controls are about identifying conditions an entity should meet or satisfy. With Chardan, either the conditions were not present or the CCO and AML Officer ignored the relevant condition. Finally, when ICBC suspended the trades for the seven companies, Chardan never investigated its customer trading activities or filed a SAR report. This fact shows that there was probably a willful breakdown in the company's controls, processes, and procedures

For CGMI, the story is different. It appears that the corporate policies, standards, controls, processes, and procedures were working correctly, but specific data never evaded the scrutiny of the compliance system. Essentially, there was no process to ensure that all the manual MMA coding was correct. Initially, no process or procedure seemed to validate the manual MMA coding. Second, on its face, the database cross-referencing was likely the correct methodology to employ. However, in general, when cross-referencing, the data in at least one of the files is assumed to be correct. If one of the files is incomplete for whatever reason, then the cross-referencing will only be a partial cross-referencing rather than a full cross-referencing. The controls that were responsible for generating the data needed to be fixed.

Another issue CGMI experienced was that the company did not test whether its advisory account database was regularly updated by the new programming of its OMS. The system analysts involved in the project likely assumed that verifying the updating process was beyond the project's scope. The project dealt with the development of the OMS, not the updating of the databases. This oversight was probably the result of a faulty requirements specification, thereby a standards issue. Finally, there were limitations in foreseeing the technological effects of the mergers in the 2008-09 timeframe. The data merger controls, processes, and procedures were likely flawed due to the systems' complexity. This situation can be particularly vexing when many of the firm's employees being merged are laid off for synergistic reasons.

For MoneyGram, as stated previously, Haider was likely either an incompetent CCO or a corrupt CCO. Nothing else can explain the blatant compliance failures experienced by the firm. It is sad, but there is nothing more to say.

The Fate of the Compliance Officers

Haider was fired on May 23, 2008.[117] As for the other CCOs, Chardan's CCO should have been for failure to act when it became known that the seven companies were likely engaging in fraud. However, the situation is different for CGMI's CCO. In general, CCOs are not technological savants. They are usually attorneys with hopefully a modicum of technological expertise. They probably do not comprehend the innards of computer systems. They must rely on seasoned systems analysts and other technological sages to provide the necessary information to perform their duties. If their experts do not fully comprehend the inner workings of a computer system or the computer system is not adequately documented, which in many instances is more than likely, there is little to nothing a CCO can do to rectify the situation. Thus, for CGMI, it is not the CCO at fault but the system analysts and computer programmers involved in maintaining and developing the compliance systems. Even so, the CCO will likely be the sacrificial lamb in this instance because the corporation needs someone to blame, and the CCO is the most likely candidate.

Compliance Surveillance Conclusion

In conclusion, this section presented three cases demonstrating CCO behavior under circumstances where the SEC accused their firms of compliance violations. In Chardan, the offending behavior involved the lack of SAR reports, likely due to customer fraud in the buying and selling penny stocks. In CGMI, the company was probably the victim of a lack of thorough data processing analysis due to either the complexity of the processing or oversight in data implications when the firm merged with other organizations, probably federally mandated as a result of the 2008-09 financial mortgage-backed securities debacle. In this instance, the CCO was more a casualty of circumstances than a willing participant in illegal behavior. It should be remembered that sacrificial lambs are usually sacrificed to appease the SEC or senior management gods when extraordinary mishaps occur. Even so, there is an argument to be made that the CCO should not be fired due to the exceptional nature of the sequence of events. It is more than likely that the CCO engaged in all reasonable steps to resolve the situation and effectively manage the compliance efforts at CGMI. Finally,

procedure#:~:text=Policies%20establish%20management's%20intent%3B,laws%2C%20regulations%20and%20frameworks)%3B.

[115] *Id.*

[116] *In the Matter of Chardan Capital Markets, LLC*, *supra*, note 2.

[117] *In the Matter of Thomas E. Haider*, *supra*, note 18.

there is Haider to consider. Based on the information contained herein, Haider was either grossly incompetent or corrupted by the offending MoneyGram agents and outlets. There are seemingly no other possible explanations for his behavior.

Thus, in addressing possible CCO malfeasance, the moral of the three stories seems to depend on the events that occurred. A potential CCO should be intimately aware of the legal risks involved in taking on the position. If a CCO has little corporate power to effect change in the compliance arena, then it seems that the best thing to do is not take the position, work to change the power structure of the position, or quit and find another line of work if it is effectively impossible or impracticable to revise the positional authority of a CCO. A CCO should not assume a position without being given the ability to effect change when necessary. The problem encountered could likely be compared to boiling a frog in a kettle of water. By the time the frog understands that they are going to be boiled to death, it is probably too late to jump out of the kettle. This is apparently the quandary of many current CCOs and probably the predicament experienced by the CCOs in the three examples above. In some instances, it may be better not to get into the kettle in the first place, but if in the kettle, closely monitor the temperature of the water, jumping out when its temperature reaches some relatively unsafe pre-specified degree.

SCENARIO INVOLVING A FAKE RETAIL ACCOUNT

This section aims to discuss a fictitious scenario of the Sheer Partners, LLC (Sheer) breach by comparing it to the breaches in In the Matter of Morgan Stanley Smith Barney, LLC (MSSB), In the Matter of R. T. Jones Equities Management, Inc. (Jones), and In the Matter of Voya Financial Advisers, Inc. (VFA). In the Sheer breach, a retail investor of Sheer reached out to the company, stating that they received an account opening document from Laughton Partners, LLC (Laughton). After reviewing the three stated breaches, the article discusses what likely happened to the Sheer investor and what Sheer should do about it. Sheer's actions involved determining whether the breach indeed occurred, who should be notified, and what the legal department should do to prepare Sheer for eventual consequences caused by the breach. The piece concludes by noting that in today's electronic world, data breaches are common and not necessarily the victim's fault. Even so, justice must be served, where the law requires that victims redouble their cybersecurity efforts while at the same time possibly paying substantial fines. It is the nature of the modern world.

In the Matter of Morgan Stanley Smith Barney, LLC

MSSB customer data was stolen by an internal employee when, between approximately December 15, 2014, and February 3, 2015, MSSB customer data appeared on at least three third-party Internet sites.[118] Around June 2011, Galen Marsh, a former MSSB employee, discovered that the authorization algorithm for the FID Select Portfolio program did not work correctly when he accessed the Account Analysis Report (AAR).[119] The algorithm should have restricted his access to customer data affiliated with the financial advisers he supported. Instead, it permitted Marsh to create a report for all MSSB customers because it failed to connect to the employee data entitlements database properly. From October 2013 to December 2014, Marsh conducted about 4,000 unauthorized customer data searches.[120]

By May 2014, Marsh began exploiting an independent vulnerability because the Bureau of Industry and Security (BIS) Portal did not possess an authorization module for its Relationship Book Analysis Report. In 2014, Marsh conducted 1,900 unauthorized searches of BIS Portal customer data. Marsh downloaded the unauthorized data that he had accessed, and copied the data to his personal home server.[121] The data breach on Marsh's personal server occurred sometime between December 15, 2014, and February 3, 2015. On December 29-30, 2014, Marsh admitted that he had accessed and downloaded confidential customer information, but he denied posting the information on the Internet. On January 5, 2015, MSSB began notifying its impacted customers of the data breach.[122]

The SEC charged MSSB with violations of Sections 15(b) and 21C of the SEA and Sections 203(e) and 203(k) of the IAA. MSSB settled the action by agreeing to censure and paying a $1 million fine.[123]

In the Matter of R. T. Jones Equities Management, Inc.

Jones employed third-party servers to store its customer data. Jones failed to institute written policies and procedures that were intended to protect customer data.[124] Presumably, Jones stored its customer data on a third-party cloud which was not named in the

[118] *In the Matter of Morgan Stanley Smith Barney LLC*, Administrative Procedure File No. 3-19793 (May 20, 2020), *available at* https://www.sec.gov/enforcement/information-for-harmed-investors/morgan-stanley-smith-barney-llc.
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *In the Matter of R. T. Jones Equities Management, Inc.*, Administrative Procedure File No. 3-16827 (Sep. 22, 2015), *available at* https://www.sec.gov/news/press-release/2015-202.

case document. Jones did not store its data in encrypted form, thereby giving a potential cybercriminal clear data. Jones was a small company with 8,000 plan participants but stored personally identifiable information (PII) on over 100,000 individuals.[125]
In July 2011, Jones found a potential cybersecurity breach at its third-party web server. Jones hired a cybersecurity consultant to confirm the attack and determine the scope of the breach. The consultant traced the attack to mainland China and that the attacker had gained full access to Jones' data.[126] This consultant could not determine the extent of the breach because the attacker had deleted the system log files. Then, Jones hired a second cybersecurity consultant to review the first consultant's report and independently determine the scope of the breach. This second consultant was unable to decide whether PII was accessed during the breach.[127]

After the breach occurred, Jones notified its customers and offered them free identity monitoring via a third-party provider. The result of the breach was that the SEC required Jones to institute various cybersecurity protections, including identity theft protection.[128] The SEC asserted that Jones had willfully violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which demanded that registered investment advisers adopt written policies and procedures that reasonably safeguard customer records and information. Finally, the SEC censured Jones and fined the organization $75,000.[129]

In the Matter of Voya Financial Advisers, Inc.

In VFA, the SEC determined that the company had failed to adopt written policies and procedures in violation of the Safeguards Rule, also known as Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) and Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), or the Identity Theft Red Flags Rule.[130] In the course of six days in April 2016, one or more individuals impersonated a VFA contractor and called VFA's technical support telephone number, asking to reset the passwords of three VFA representatives. In two of the calls, the telephone numbers used by the attackers had been previously identified as being affiliated with fraudulent activity.[131] The VFA staff reset the passwords and provided the attacker with temporary passwords and the representative's username. About three hours after the password reset, the actual contractor informed VFA that they had received a confirmation email stating that their password had changed, even though they had not requested the change. The intruders employed this new-found information to access the PII of at least 5,600 VFA customers. The attackers also used the information that they obtained to create new VFA customer profiles.[132]

VFA violated the Safeguards Rule because its cybersecurity policies and procedures did not include a data breach using contractor information as a source of a breach. Although VFA had adopted an identity theft program in 2009, the SEC opined that the policies and procedures were not designed to deal with identity theft red flags that were detected during this breach. After VFA detected the breach, it instructed technical support to no longer provide temporary passwords via a telephone call.[133]

The result of VFA's conduct was that the SEC charged the company with willfully violating Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) and Rule 201 of Regulation S-ID (17 C.F.R. § 248.201). VFA consented to various SEC recommendations. The firm was censured and fined $1,000,000.[134]

The Situation at Sheer Partners, LLC

The situation at Sheer is that a retail investor reached out to the company, stating that they received an account opening document from Laughton. However, the investor never opened an account at Laughton. The only investment account the investor had was with Sheer.

The retail investor at Sheer is likely reporting to Sheer that a data breach has occurred. The Sheer network had probably been breached. Based on the information contained above, there were three possible ways that intruders were able to access PII from the Sheer system. First, based on the MSSB case, Sheer customer data could have been breached by an internal employee for their own purposes, likely to sell Sheer customer data to an unknown third party. Second, assuming that the Jones case is applicable, the breach could have occurred because Sheer was using a third-party server (likely a cloud facility) to store and process customer data. Third, according to the VFA case, the Sheer customer data could have been breached when the intruders employed social engineering techniques to gain access to the Sheer system. This social engineering could have been as simple as calling VFA customer support and impersonating an individual who has access to the VFA system but forgot their password. The VFA customer support staff could have innocently provided the intruder with a temporary password over the telephone or via email.

---

[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *In the Matter of Voay Financial Advisers, Inc.*, Administrative Procedure File No. 3-20183 (Dec. 21, 2020), *available at* https://www.sec.gov/files/litigation/admin/2020/34-90745.pdf.
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.*

It should be remembered that these three intrusion possibilities mentioned above may not have been the only ways that cybercriminals could have gained access to Sheer customer data. For example, the intruders could have used a man-in-the-middle (MITM) attack, in which they captured the investor's information while the investor was logged into the system.[135] With an MITM attack, or an on-path attack, an attacker secretly captures and then relays a communication between two parties who believe that they are directly communicating with each other. The attacker has implanted themselves between the two parties and collected their information.[136] Another possibility is that the attacker employed social engineering to obtain access to one customer account and then used an Structured Query Language (SQL) injection technique to obtain information on every Sheer customer.[137] An SQL injection occurs when an attacker injects malicious SQL code into an application, permitting the attacker to see or change a database.[138] In this instance, the cybercriminal would likely have obtained all Sheer customer data, and then used that data to open an account at Laughton. The Laughton system would then have innocently sent the investor a letter confirming that the investor had opened up a Laughton account.

What Is to Be Done

Once the investor had informed Sheer that they had received a letter from Laughton confirming the opening of a Laughton account, the Sheer employee receiving this information should have issued an alert to Sheer customer support, cybersecurity, and legal departments, as well as informing their manager and possibly senior management. One thing that the Sheer employee should do is verify with the investor whether they had forgotten that they had previously opened a Laughton account. It is possible that the investor was mistaken, and that the investor's call to Sheer was a false alarm.

With this information from the investor and assuming that no false alarm happened, the cyber security department would be responsible for verifying that a breach had actually occurred and the extent of the breach. This may take some time to do. In the meantime, the attacker may be using this recognition delay to steal more Sheer customer data. The question that Sheer Cybersecurity must ask itself is whether the delay in reporting the incident is acceptable. It is probably reasonable to verify the existence of a breach rather than report a false positive to the appropriate government agencies, provided that the delay in reporting is not extensive (i.e., several months).

Once Sheer Cybersecurity has verified that the data breach is genuine, this information should be relayed to Sheer senior management and its legal department. Senior management then has the responsibility of informing Sheer customers of the data breach, while suggesting efforts that they can take to reduce the effect of the breach. For example, Sheer senior management could suggest that Sheer customers change their passwords. If Sheer is employing two-factor authentication, Sheer customers would likely have to change their password and the two-factor authentication criteria that Sheer customers employ. This would be a necessary inconvenience for Sheer customers.

Senior managers should also inform the appropriate government agencies of the breach and the steps that they are taking to resolve the matter. If at all possible, Sheer senior managers should relay to the government and its customers the extent of the breach. It should be remembered that this number is an estimate that likely understates the extent of the breach. More accurate numbers are likely to emerge as the Cybersecurity department further analyzes how the breach occurred and what was taken.

Although not necessarily immediately, Sheer senior managers should institute a process of evaluating its cybersecurity policies, standards, controls, processes, and procedures. The reason for this analysis is to estimate what failed and how the cybersecurity mechanisms need to be changed. This effort is not a short-run endeavor. It may take months to determine where the failure occurred and what additional steps should be taken to ensure that the breach does not happen again. Even so, Sheer senior management is faced with the prospect of another data breach occurring sometime in the future, if only due to the fact that human beings are not infallible creatures. Human beings make mistakes, and there is no way around it. As Irish poet Robert Burns so aptly put it, " The best-laid plans of mice and men often go astray."[139]

The legal department is responsible for estimating Sheer's estimated liability. This can be achieved using the Program Evaluation Review Technique (PERT) three-point estimation technique. The formula is:[140]

Expected Liability = (Optimistic Liability + 4 * Most Likely Liability + Pessimistic Liability) / 6

---

[135] Kinzer Yasar, Man-in-the-Middle Attack (MitM), *Tech Target* (Apr. 2022), *available at* https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.

[136] *Id.*

[137] Bart Lenaerts-Bergmans, SQL Injection (SQLI): How to Protect Against SQL Injection Attacks, *Crowd Strike* (Oct. 10, 2022), *available at* https://www.crowdstrike.com/cybersecurity-101/sql-injection/.

[138] *Id.*

[139] Robert Burns, To a Mouse, *Poetry Foundation* (n.d. [Nov. 1785]), *available at* https://www.poetryfoundation.org/poems/43816/to-a-mouse-56d222ab36e33.

[140] Ina Grozeva, PERT Estimation: The Key to Successful Project Planning and Management, *DevStride* (n.d.), *available at* https://www.devstride.com/blog/pert-estimation-the-key-to-successful-project-planning-and-management#:~:text=The%20three%20estimates%20are%20then,accurate%20estimate%20for%20the%20task.

For example, if the optimistic liability is $100,000, the most likely liability is $500,000, and the pessimistic liability is $1,000,000, then the expected liability is:
Expected Liability = ($100,000 + 4 * $500,000 + $1,000,000) / 6 = $516,667
Once the qualitative optimistic liability, most likely liability, and pessimistic liability estimates are specified and the calculation is accomplished, the Sheer legal department should inform senior management of the results of the calculation. If the Sheer breach was more like the Jones breach, the fine would likely be under $100,000. On the other hand, if the Sheer breach was similar to the MSSB or VFA breaches, Sheer should expect the fine to be at least $1 million. Sheer senior management is responsible for setting aside at least the calculated expected liability to be paid as a fine to the federal government, and possibly several state governments.

Fake Retail Account Conclusion

In conclusion, Sheer is likely in a no-win situation. The fact that the breach occurred does not indicate that the company did not previously take positive steps to prevent the breach from occurring. In today's world, where data breaches are common, cybercriminals may attempt to steal an organization's data despite what a company does to prevent it. After examining the three cases above, the SEC seems eager to categorize any data breach as an indication of willful and unreasonable behavior on the part of an organization. This attitude is not necessarily correct. Even so, we live in a litigious world where blame must be ascribed to show the public that the government is protecting them. It is the nature of the world we currently live in.

SOCIÉTÉ GÉNÉRALE AND THE JÉRÔME KERVIEL SCANDAL

This section discusses the SocGen scandal and whether Jérôme Kerviel was the sole culprit or whether he was formatted and distorted by SocGen. The piece dissects the case against Kerviel, pointing out that the French courts ultimately ruled that it was SocGen, not Kerviel, who was responsible for the financial debacle. The corrective actions that could have prevented the €4.9 billion loss were seemingly rather simple. SocGen likely had comprehensive compliance policies and procedures in place. The fact that the company did not follow its policies and procedures indicates that their lust for money overcame their integrity and better judgment. As a young individual just out of college from a working-class family, Kerveil was driven to be successful and probably succumbed to SocGen's culture of greed. The French courts apparently agreed with the previous statement. Thus, the section concludes that the moral of the story is that if a firm possesses reasonably adequate compliance policies and procedures, it should follow them, thereby foregoing quick profits and enduring to the end.

The Facts of the Case

Kerviel was a junior derivatives trader for SocGen, a French securities firm.[141] Kerviel was hired to work in the Middle Office or the compliance department of SocGen in 2000.[142] In 2005, Kerviel was promoted to the Delta One products team, which was located in Paris,[143] where he became a junior trader.[144] Delta One's business included exchange-traded funds, index futures, program trading, quantitative trading, and swaps. Kerviel's role at Delta One was to ensure that SocGen profited from discrepancies between equity derivatives and the underlying market price of the derivative-based stocks.[145] In 2006, Kerviel's base salary was about €74,000 with a €60,000 bonus; in 2007, Kerviel had hoped for a €600,000 bonus.[146]

Because Kerviel had spent five years in the SocGen compliance department, he was well acquainted with corporate policies for approving and regulating the trading activities of its brokers.[147] From late 2006 to early 2008, Kerviel exploited his knowledge of the bank's Middle Office by offsetting his one-sided trades with bets in the opposite direction, employing fake computerized trades not flagged by SocGen's oversight system.[148] [149]

---

[141] James Chen, Jerome Kerveil: A History and Work with Derivatives, *Investopedia* (Jum. 26, 2022), *available at* https://www.investopedia.com/terms/j/jerome-kerveil.asp.
[142] Ben Martin, Nick Allen, Peter Allen, & Henry Samuel, Jerome Kerviel was 'honest, working class', *The Telegraph* (Jan. 28, 2008), *available at* https://web.archive.org/web/20080203164327/http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/26/nkerviel426.xml.
[143] Gordon Rayner and Peter Allen, Profile: Rogue Trader Jerome Kerviel, *The Telegraph* (Jan. 26, 2008), *available at* https://web.archive.org/web/20080128064429/http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2008/01/25/nsocgen325.xml.
[144] James Mackenzie, & Andrew Hurst, French Trader Kerviel Cooperating with Police, *National Post* (Jan. 26, 2008), *available at* https://archive.ph/20080128055324/http://www.nationalpost.com/news/story.html#selection-731.0-731.45.
[145] James Chen, supra, note 1.
[146] Christine Sieb, Societe Generale missed 75 warnings on trader Kerviel, *The Times* (Feb. 21, 2008), *available at* https://www.thetimes.com/article/societe-generale-missed-75-warnings-on-trader-kerviel-xvzc27f09dn.
[147] James Chen, *supra*, note 1.
[148] *Id.*
[149] Christine Sieb, *supra*, note 6.

In January 2008, SocGen management began to unwind Kerviel's position, with losses estimated at €4.9 billion, whereas in the previous year, Kerviel generated €1.4 billion in profits.[150] Kerviel asserted that the bank's senior management was aware of the riskiness of Kerviel's trades, but did nothing, looking the other way because of the profits that he generated.[151]

In 2010 and before his trial, Kerviel wrote a book entitled L'Engrenage: Mémoires D'un Trader or The Vicious Spiral: Memories of a Trader.[152] In that same year, Kerviel was convicted of breach of trust and other charges,[153] sentenced to three years in prison and was required to pay a €4.9 billion fine.[154] During the trial, Kerviel maintained that although he faked trades, he hid nothing from his supervisors.[155] Kerviel appealed the decision, and in 2016, an appellate court in Versailles opined that Kerviel's behavior was due to SocGen's managerial choices, which allowed the trader to commit criminal acts.[156] In June 2016, A French labor court ordered SocGen to pay Kerviel €450,000 in damages, opining that the former trader was wrongfully dismissed without genuine or serious cause because the bank knew about his dealings.[157] In September 2016, Jolly and Grant reported that an appeals court in Versailles reduced Kerviel's fine to €1 million, including damages and interest.[158] The net effect of this ruling was that Kerviel only owed SocGen €550,000 (= €1 million – €450,000). In the end, according to Langworth, Kerviel wanted to make a name for himself as a star trader, escaping from his lowly status at SocGen and from the trauma of his personal life, where his father died in 2006, and his marriage disintegrated in 2007.[159] As of Langworth's article, Kerviel was an IT consultant.[160]

Potential Corrective Actions

The possible corrective actions depend on whether the blame for SocGen's €4.9 billion loss should be placed squarely on Kerviel's shoulders or whether SocGen is a victim of its insatiable greed. The French courts have resoundingly answered this question. SocGen is responsible for Kerviel's behavior because it failed to curtail his trading activities. Now, it should be remembered that Kerviel spent five years in SocGen's Middle Office or compliance department. It was during these five years that Kerviel came to understand SocGen's policies and procedures thoroughly. When Kerviel was promoted to Delta One, the advantage that he possessed over the other traders was that he was well-versed in the company's compliance policies and procedures. He had the opportunity to view first-hand the limits and nuances of these policies and procedures. He discovered that SocGen's policies and procedures should be satisfied at the end of each trading day, not necessarily at any time during the day.[161] This may have been a competitive advantage, presuming that the other traders in Delta One were aware of it. It should be remembered that Kerviel stated that he was one of the individuals who predicted the subprime crash of 2008. He may have become engrossed in the idea that the subprime market would crash and he and SocGen would make volumes of money.[162]

According to Kerviel, his supervisors deactivated the alerts system, removing all the safeguards from his computer.[163] If so, and the decision from the French courts seems to point in this direction, then corrective actions are SocGen's responsibility. The critical issue is that if a company fails to adhere to its compliance policies and procedures, it is not Kerviel's fault that he is allowed to make these trades. According to the court, the blame lies at SocGen's feet. The moral is, therefore, to adhere to compliance policies and procedures, not ignore them when sugar-plum profits are dangled in the corporation's face.

---

[150] BBC Staff, Rogue Trader Began Year in Profit, *BBC News* (Jan. 30, 2008), *available at* http://news.bbc.co.uk/1/hi/business/7218380.stm.
[151] *Id.*
[152] Courtney Comstock, Rogue Trader: Feel Bad for Me, I Was Just a Prostitute in the Banking Orgy, *Business Insider* (May 3, 2010), *available at* https://www.businessinsider.com/jerome-kerveil-feel-bad-for-me-i-was-just-a-prostitute-in-the-banking-orgy-2010-5.
[153] James Chen, *supra*, note 1.
[154] CNN Wire Staff, France's Biggest Rogue Trader to Serve 3-Year Prison Term, *CNN News* (Oct. 24, 2012), *available at* https://www.cnn.com/2012/10/24/world/europe/france-trader-case/index.html.
[155] Gregory White, Jerome Kerviel: I Faked Trades, *Business Insider* (Jun. 9, 2010), *available at* https://www.businessinsider.com/jerome-kerviel-i-faked-trades-2010-6.
[156] James Chen, *supra*, note 1.
[157] Cynthia Kroet, Rogue Trader Jérôme Kerviel Wins Unfair Dismissal Claim, *Politico* (Jun. 7, 2016), *available at* https://www.politico.eu/article/rogue-trader-jerome-kerviel-wins-unfair-dismissal-claim-societe-generale/.
[158] David Jolly, & Nicola Clark, Ex-Société Générale Trader's Huge Fine Is Cut to 1 Million Euros, *The New York Times* (Sep. 23, 2016), *available at* https://www.nytimes.com/2016/09/24/business/international/jerome-kerviel-societe-generale-fine.html.
[159] Hannah Langworth, Rogue Traders: Jerome Kerviel, *Trader Life* (n.d.), *available at* https://traderlife.co.uk/series/rogue-traders/rogue-traders-jerome-kerviel/#:~:text=Though%20Kerviel%20would%20never%20become,career%20as%20an%20IT%20consultant.
[160] *Id.*
[161] Courtney Comstock, Jerome Kerviel: "Jerome Kerviel had to be 'shot down.'", *Business Insider* (Nov. 16, 2010), *available at* https://www.businessinsider.com/the-greatest-interview-jerome-kerviel-has-ever-given-2010-11.
[162] *Id.*
[163] *Id.*

One issue that should be discussed is whether a trader can exceed the compliance limits during a trading day, provided the limits are met at the end of the day. There are reasonable arguments to suggest that trading limits should be enforced throughout a trading day. However, equally good arguments support the notion that as long as the trading limits are satisfied at the end of the day, little to no harm has been done.

Finally, it should be remembered that after Kerviel's trades were "discovered," the company unwound them in three days. This action likely occurred because SocGen management feared for the bank's existence. The action further destabilized the derivatives market by giving traders the impression that a coming crash was likely. Had the bank understood that a subprime crash was coming, SocGen might have experienced significant profits, much like Michael Burry and Mark Baum did, as exemplified in the movie entitled The Big Short.[164] As for SocGen, the French government indicated that it would reclaim SocGen's €2.2 billion tax deduction if the appellate opined that Kerviel was not responsible for the losses that he incurred.[165]

Société Générale and Kerveil Conclusion

In conclusion, it appears that Kerviel was a victim of overly zealous SocGen management that valued profits over compliance. The lure of easy money may turn even the saintliest organization into an entity hell-bent on profits. The key is to have thorough and fair compliance policies and procedures and then adhere to them under all circumstances. Here, enduring to the end is what matters.

ISSUES WHEN HIRING AN INVESTMENT ADVISER

The section discusses a fictitious scenario where the due diligence conducted by a compliance officer in hiring an individual with 30 years of experience at presumably another broker/dealer as an investment adviser. Some of the issues described herein are directly related to compliance, while others are only peripherally affiliated. The section begins by stating the situation and asking a sequence of questions. In the second section, the piece highlights what can happen because of a "bad hire," defines due diligence in this context, and lists four factors that should play into the hiring process. If complaints about the candidate are discovered, the section argues that the nature of the complaints should be assessed. It is impossible to go through life unscathed. Finally, the piece concludes by observing that although there are risks in hiring an older candidate, there are risks associated with onboarding a candidate, say, fresh out of college. Young people tend not to have an extensive history, and their behavior may be unknown. There is a risk, no matter what choice is made. It is the nature of the decision.

It should be noted that the individual was likely not an investment adviser at their previous position. What were the duties of this individual at their previous position? Did they have any customer experience? If so, how much experience? If not, why not? In other words, was the individual involved in making trades for customers, did they work in the back office where they had little or no customer experience, or did they work in some other department, such as the information technology (IT) department as a computer programmer? After 30 years performing specific activities for a company, an individual would want to exploit their competitive advantage and continue doing the same line of work, say perhaps until they retire. The fact that the person wants to change their occupation could be construed to be a red flag or at least an issue that begs for a reasonable explanation. Finally, when deciding to apply for the position of investment adviser, does the individual possess the necessary licenses required by the various regulatory bodies to be hired as an investment adviser? If so, the hiring process will likely proceed, but if not, it might be a better idea to advise what tests need to be passed so that they may qualify for the position at some future date and possibly at some other firm.

Due Diligence and Best Hiring Practices

According to Kluttz, a bad hire can occur if a new hire succeeds in misdirecting or lying to an interviewer.[166] It is also possible that critical information regarding an individual is neither requested nor acted upon.[167] A bad hire can be painful or costly due to:[168]

- Attrition and wasted hiring budgets;
- Theft or embezzlement;
- Damaged employee relations and morale;
- Endangerment of employees, clients, and business associates;
- Lost productivity;
- Litigation; or

[164] THE BIG SHORT (Adam McKay dir. 2015).
[165] Jean-Baptiste Vey, & Richard Lough, French Govt Indicates Will Reclaim SocGen Tax Deduction If Trader Wins Case, *Reuters* (Sep. 23, 2016), *available at* https://www.reuters.com/article/socgen-kerviel/french-govt-indicates-will-reclaim-socgen-tax-deduction-if-trader-wins-case-idUSL8N1BZ0OP/.
[166] Melissa Kluttz, Employee Due Diligence for Financial Services Industry, *Sterling* (Aug. 23, 2018), *available at* https://www.sterlingcheck.com/blog/2018/08/due-diligence-financial-services-industry-best-practices/.
[167] *Id.*
[168] *Id.*

- Public scandals and negative publicity.

According to the Merriam-Webster Dictionary, due diligence is the "care that a reasonable person exercises to avoid harm to other persons or their property."[169] Chen defined due diligence as an "investigation, audit, or review performed to confirm facts or details of a matter under consideration."[170] In the financial industry, due diligence demands that financial records are examined before a proposed transaction is consummated.[171] In this instance, due diligence might require the firm to evaluate the previous company's employment records, such as employee reviews by their manager. In other words, due diligence is the reasonable steps an individual or company takes to satisfy a legal requirement, such as buying or selling something. In this instance, the firm purchases the candidate's time and possible work product or expertise.

When hiring a candidate, regardless of their previous experience, a company should obtain and verify, among other things, an individual's:[172]

- Education and work history;
- Industry qualifications, certifications, and licenses;
- Criminal and fingerprinting records;
- Credit checks;
- Disciplinary information; and
- Outside business activities.

The idea behind adequate due diligence is to discover material "skeletons" in a candidate's closet. This may be difficult to obtain if the "skeletons" are old and not adequately documented.

The four key factors that the firm should consider when performing its due diligence regarding the candidate include:[173]

- **Data Collection –** The company should possess a comprehensive process that results in a detailed risk profile of the candidate;
- **Verification –** Initial and continued interviewing and investigating, although time-consuming, will likely help the firm create clear and accurate information regarding real or perceived conflicts of interest, criminal activity, or regulatory issues.
- **Monitoring –** The firm should have an ongoing monitoring tool to expose factors that may be missed by traditional monitoring methods, such as criminal activity, liens and judgments, etc. to obtain a complete picture of the candidate;
- **Obtaining and Verifying Information –** There is a need for candidate self-reporting, but the company's verification efforts should be supplemented by obtaining:[174]
  - Outside business activities (OBA) certifications;
  - Anti-money laundering (AML) checks;
  - Due diligence questionnaire responses;
  - Credit reports;
  - Criminal background checks and arrest records;
  - Lien and judgment data; and
  - Educational institutions and certifications information.

Collecting this information can be a lengthy process. It is possible that the candidate will not wait for the process to finish. They may seek opportunities elsewhere. Thus, depending on the quality of the candidate, there is a balance to be struck between gathering the requisite information and the hiring decision. Sometimes, much of the information about an individual is publicly known, meaning that the investigative process could be curtailed. Finally, collecting information about a candidate should not violate the person's right to privacy. It is preferred that the firm ask the individual to consent to an investigative background check so that their privacy rights are not abridged.

What to Do If There Were Complaints

Working 30 years for a broker/dealer, there are bound to be some complaints. No one comes out of a 30-year experience unscathed unless they never had the opportunity to provide financial advice or implement trades for another person. It should be remembered that even janitors can be the subject of unfavorable reviews. The burning question is what the individual did or did not do that precipitated a complaint.

---

[169] Due Diligence, *Merriam-Webster Dictionary* (n.d.), *available at* https://www.merriam-webster.com/dictionary/due%20diligence.
[170] James Chen, Due Diligence, *Investopedia* (Jan. 18, 2024), *available at* https://www.investopedia.com/terms/d/duediligence.asp.
[171] *Id.*
[172] Melissa Kluttz, *supra*, note 166.
[173] *Id.*
[174] *Id.*

Thus, when examining a person's employment and personal information, the company should be careful as to what information is deemed critical, thereby preventing hiring. Even convicted felons can be hired under some circumstances. For example, in the movie Wall Street: Money Never Sleeps, Gordon Gekko (Michael Douglas), who was imprisoned for eight years for insider trading and mail fraud, did business with Julius "Julie" Scherhart (Eli Wallach) because he "[spoke] to [Scherhart's] materialistic business clients in the language they understand and respect: by correctly predicting the coming financial collapse."[175]

However, in this instance, the candidate is likely not as notorious as Gekko, but even so, their financial expertise may be worth hiring, provided that a certain amount of remorse and transparency exists. The more probable scenario is that the candidate had a low to medium-level position at their previous company, and there were some complaints, but not necessarily earthshaking. Here, it may be worth hiring the candidate, particularly if they want to get out of the hum-drum of their previous employment situation and try something new. If the candidate dares to begin again and go through the rigors of starting over in a new occupation, they may positively contribute to the organization.

There is one caveat that needs to be addressed. The candidate has 30 years of experience with another broker/dealer. The hiring process should not discount the individual based on their age. If the firm makes the mistake of not hiring the candidate because it wants "young blood," the company may be opening itself up for an age discrimination suit, which can turn out to be rather expensive.

Hiring an Investment Adviser Conclusion

Thus, care should be taken when onboarding the candidate. They should be treated like any other candidate for the position, except their expertise at their previous broker/dealer should enter into the hiring calculation. Remember that when a company hires a candidate young in years, they are an open book that has yet to be written. There is a risk that a young candidate may deviate from established norms to solidify their position at the firm and in the industry. With an older candidate with extensive experience, the firm will likely know who it is getting if it hires the person. There is always a risk in onboarding someone. The issue is, what are the risks that a firm is willing to take?

SCENARIO INVOLVING UNAUTHORIZED TRADES

This section dissects the compliance issues associated with the following fictitious scenario. Lauren filed a complaint with the compliance officer, alleging that Edward, a registered representative at the firm, recently conducted three trades without the customer's authorization. During the call with Lauren, she stated that when she looked at her account statement, she saw some weird investments in Company X, which the compliance officer knew was a newly established software company.

Following this introduction, the facts of the scenario are listed. The next section asks eight questions, the answers of which will determine what the compliance officer recommends to the broker/dealer's senior management and corporate counsel. The third section talks about due diligence issues in general. The fourth section asks whether the firm should file a SAR with FinCEN. The fifth section lists possible recommendations to senior management and corporate counsel. The section concludes by pointing out that the scenario is not necessarily as straightforward as it seems. The compliance officer's response differs based on possible additional facts absent from the scenario. The actions range from compensating the customer for losses, if appropriate, to reporting the registered representative to various regulatory agencies as a subject of possible criminal action.

Issues with the Scenario Facts

In this section, eight questions are asked and answered regarding the stated scenario. The first question asks who is Lauren. Although the scenario seems to presume that she is a broker/dealer customer, it is not specifically stated. The actions taken by the broker/dealer depend on who she is, her position, and her relationship with the firm. The second question asks whether the alleged three trades happened. The existence of the three transactions should be verified so that the investigation can proceed. The third question suggests that Lauren may have forgotten that she previously authorized the trades. If so, Edward may have done nothing wrong, which would have furthered the investigation. The fourth question observes that Lauren may have made the trades herself; the trades went bad, and she is looking for a scapegoat. Although not likely, this option should not be discounted.

The fifth question deals with the possibility that Edward mistakenly made three incorrect trades. In this instance, there was likely no intent to deceive or profit fraudulently. However, some discipline of Edward is probably in order. This sixth question suggests that Lauren may have authorized the three trades under duress. If so, the follow-up question is: who was the source of the duress? This is an important issue to resolve, for the source may be Edward or an undisclosed third party. The seventh question is concerned with whether Lauren had legal capacity at the time that the trades were made. It is possible that the transactions were implemented at the direction of Lauren's legal guardian and that she is currently disavowing responsibility for the trades after turning 18 years old. The final question asks whether the three trades were legal at the time of the transaction and became illegal shortly after. Edward is guilty of facilitating illegal trades if they were illegal when the transaction was consummated. On the other hand,

[175] Wall Street: Money Never Sleeps – Plot, *Internet Movie Data Base (IMDB.com)* (n.d.), *available at* https://www.imdb.com/title/tt1027718/plotsummary/?ref_=tt_stry_pl.

if the trades were initially legal and then became illegal, Edward is likely free of legal liability, and Lauren may be seeking to cover her losses by reporting the incident to the compliance officer.

Who Is Lauren?

Various questions should be asked and answered when examining this scenario's information. Who is Lauren? Is Lauren a customer or an employee of the broker/dealer? For this section, it will be assumed that Lauren is one of the broker/dealer's clients. However, if Lauren was an employee of the broker/dealer and the account belonged to her, it would again be correct to presume that she is a broker/dealer client. Suppose Lauren was the registered representative's supervisor, and the account belonged to an undisclosed third party. In that case, why did Lauren authorize the investment of Company X, a newly established software company? In this instance, the undisclosed third party may have authorized the purchase of Company X stock. Suppose Lauren must authorize the stock purchase for and on behalf of an undisclosed third party. What are the relationships among Lauren, Edward, and the undisclosed third party? It could be that Edward is merely an intermediary executing trades on command. Thus, from now on, it will be assumed that there is no undisclosed third party. Lauren is the client, and Edward made trades on her account.

Did the Trades Actually Occur?

It should be verified that the trades occurred and Edward made those trades. It is possible that the trades never happened or that some of the three trades were made, but others were not. Also, if the three trades were made, an obvious question is whether they were all buy trades or some buy and some sell trades. It is possible that there were three buy trades, two buy trades, and one sell trade, or one buy trade and two sell trades. Three sell trades would imply that Lauren had previously owned stock in Company X. No matter what was the sequence of trades, one issue that should be examined is whether, after the three trades were consummated concerning the stock of Company X, did Lauren still own any shares of Company X? If so, the compliance officer should ask Lauren if she wants to keep or sell these outstanding shares. Lauren may want to keep the shares, or she may want to sell them.

Did Lauren Forget that She Authorized the Trades?

Assume that Lauren did not authorize Edward's three trades. It could be that Lauren forgot that she had authorized Edward to make those trades. If so, there may or may not be written confirmation of the previous authorization. Lauren may have given Edward verbal authorization to make the trades, and now, for some reason, has forgotten her previous instructions. When prompted, Lauren may remember her previous authorization, in which Edward faithfully followed her instructions, and there is no compliance issue, except that Edward should have a written record of Lauren's authorization. It should be remembered that if Edward has no written record that he was authorized to make the trades. This may be a red flag of unauthorized activity.

Did Lauren Make the Trades Herself?

These days, Lauren could have made the trades herself through the broker/dealer's website. The trades could have resulted in a substantial loss Lauren did not want to experience. Because she had previously worked with Edward on previous trades, Lauren could have concocted the idea of blaming Edward for her losses. Although this explanation may be unlikely, it is not outside the range of possibility. The compliance officer should not be so naïve as to assume Lauren is telling the truth. She may be lying to cover up her actions.

Did Edward Make a Mistake in Executing the Trades?

It is possible that Edward was instructed to buy or sell Company Y's stock rather than Company X's stock. It may be that the CUSIP symbols are so close to one another that Edward mistook one stock for another. If so, this issue is squarely in Edward's lap, assuming that he previously had the authority to make trades for and on Lauren's behalf. What could have occurred was a communication error between Lauren and Edward. In this instance, there was likely no intention to commit a crime. The firm could reimburse Lauren for any losses that she incurred. The broker/dealer could also offer to purchase Company's X stock at the price she paid, leaving Lauren financially unharmed.

Did Lauren Authorize the Trades under Duress?

It is possible that Lauren authorized the three trades under duress. The duress could have originated from Edward or an undisclosed third party. This behavior would probably have been unethical and illegal if Edward had placed Lauren under duress. However, if the duress came from an undisclosed third party, that individual could be Lauren's friend, relative, or associate. If so, Lauren may be accusing Edward of executing three unauthorized financial transactions to shift blame from her friend, relative, or associate to Edward to protect them from possible legal action.

Did Lauren Have the Capacity to Authorize the Trades?

Although the scenario does not explicitly say so, Lauren could have been a minor when the trades were executed. It is possible that her legal guardian authorized Edward to make the three trades. Now, Lauren has just turned 18 years of age and is disavowing the trades. She may be accusing Edward of making the three unauthorized trades because she does not realize that, as a minor, she did not have the legal capacity to authorize the trades. Lauren may be accusing Edward of making three unauthorized trades because she needs a scapegoat to take the blame for the actions of her guardian.

Were the Trades Legal at the Time of the Transaction?

It is possible that Lauren either authorized Edward to make the three trades or made the trades herself, but the trades were either illegal at the time or became illegal shortly thereafter. Lauren may feel that Edward was responsible for the trades because he should have instructed her of their likely illegality or coming illegality. If so, Edward is responsible only if he executed the trades knowing they were illegal. He is not responsible if the trades were legal when they occurred but became illegal shortly after that. There may have been no way for Edward to anticipate the coming illegality of the trades. According to the scenario, Edward was a registered representative (Series 6), although his more likely title was an account executive (Series 7). It should be remembered that a registered representative is only authorized to sell mutual funds, variable annuities, variable life insurance, unit investment trusts (UITs), and municipal fund securities,[176] whereas an account executive can buy and sell individual stocks and bonds, UITs, real-estate investment trusts (REITs), government securities, options, hedge funds, venture capital, mutual funds, etc.[177] In other words, an individual who holds a Series 7 license can do all the transactions that a person holding a Series 6 license can do and more.

Due Diligence Issues

Again, the four critical factors that should be considered when a company conducts its due diligence are:[178]

- **Data Collection –** There should be a comprehensive process that generates a detailed risk profile of an employee;
- **Verification –** Although initial and continued interviewing and investigating are time-consuming, they will probably assist the company in establishing clear and accurate information regarding actual or perceived conflicts of interest, criminal activity, or regulatory issues.
- **Monitoring –** The company should have a tool that exposes factors such as criminal activity, liens, judgments, etc., to obtain a complete picture of the candidate;
- **Obtaining and Verifying Information –** Presuming that employees self-report issues, the firm's verification efforts should be augmented by attaining:[179]
    - OBA certifications;
    - AML checks;
    - Due diligence responses;
    - Credit reports;
    - Criminal background checks and arrest records;
    - Lien and judgment data; and
    - Education and certifications information.

Procuring this information can be an arduous process. It is possible that Edward will not wait for the process to finish. He may seek opportunities elsewhere. There is a balance to be struck between gathering the requisite information and the termination decision. Sometimes, much of the information about a person is publicly known, meaning that the investigative process could be curtailed. Finally, collecting information about an employee should not violate the person's right to privacy. It is preferred that the firm ask the individual to consent to an investigation so that their privacy rights are not abridged.

Filing a Suspicious Activity Report

Presuming that Edward made three unauthorized trades for Lauren, the question arises as to whether the broker/dealer should file a SAR with the appropriate federal agency. A SAR report is a "document that financial institutions, and those associated with their business, must file with the FinCEN whenever there is a suspected case of money laundering or fraud."[180] A SAR report monitors any unusual or potentially illegal activity within the financial industry that could threaten public safety.[181]

The first thing that the compliance officer should do is consult with the broker/dealer's legal department. If the legal department recommends filing a SAR report, the compliance officer must file the report. However, suppose the legal department suggests that the compliance officer does not file a SAR. In that case, there is a risk that the appropriate federal agency may disagree with the legal department's advice. To be conservative, the compliance officer should likely seek a second opinion from an individual

[176] FINRA Staff, Series 6 – Investment Company and Variable Contracts Products Representative Exam, *Financial Industry Regulatory Authority* (2024), *available at* https://www.finra.org/registration-exams-ce/qualification-exams/series6.
[177] FINRA Staff, Series 7 – General Securities Representative Exam, *Financial Industry Regulatory Authority* (2024), *available at* https://www.finra.org/registration-exams-ce/qualification-exams/series7.
[178] Melissa Kluttz, *supra*, note 166.
[179] *Id.*
[180] Thomspon Reuters Staff, What Is a Suspicious Activity Report?, *Thompson Reuters Legal Solutions* (2024), *available at* https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report#:~:text=A%20Suspicious%20Activity%20Report%20(SAR,of%20money%20laundering%20or%20fraud.
[181] *Id.*

not affiliated with the federal agency. It is also a good idea for the compliance officer to conduct their own research as part of the decision-making process.

Recommendations to Senior Management and Corporate Counsel

The recommendations to senior management and corporate counsel depend on what is uncovered during the investigation. There may be little or no action to recommend. or there may be significant proposals to consider, including legal action against the registered representative. If it is determined that the registered representative illegally and unethically made three unauthorized trades in the individual's account, the broker/dealer could be subject to legal action by Congressionally empowered federal agencies, resulting in millions of dollars in fines. The idea is to suggest that the broker/dealer be transparent to minimize legal liability.

Unauthorized Trades Conclusion

In conclusion, the scenario is more complex than it seems. The compliance officer should answer various questions before concluding that Edward illegally and unethically made trades in Lauren's trading account. The issues brought up herein are reminders that things may have deeper meanings. Factors could indicate a vastly different response based on what actually occurred. It may turn out that the prima facie case is correct, but then again, there may be unstated issues that point to a distinctive reaction. The compliance officer must be somewhat skeptical regarding the information Lauren presented. The solution resides in the paper trail of the three trades and Edward's testimony. It should be remembered that if Edward truthfully states that he was under orders from Lauren or her guardian to make the three trades, and the broker/dealer dismisses Edward out-of-hand, it may be facing a lawsuit. There is no royal road here, no easy solution. It is only by diligent investigation that the truth will likely emerge.

CONCLUSION

This article was broken up into nine major sections. The first section specified financial compliance definitions, including a fiduciary, a fiduciary's standard of care, and a broker/dealer, discussing whether a broker/dealer is a fiduciary and the relationship between the SEC and the fiduciary standard of care. The second section dealt with CPR and its application to Merrill Lynch's misuse of customer funds, where the company did not deposit customer cash in a reserve account, thereby putting customer money at risk in the event of bankruptcy. The third section concerned the five AML pillars, including designating a compliance officer, completing risk assessments, building internal controls and AML policies, monitoring and auditing an AML program, and performing CDD. The third section evaluated MSSB and the UBS subsidiaries UBSFS) and UBSS AML cases.

The fourth section was a fictitious scenario in which a registered representative for a broker/dealer used their personal email to communicate with customers about business-related matters. The scenario explored under what circumstances the registered representative violated FINRA rules. The fifth section discussed three financial compliance surveillance cases, demonstrating that financial compliance can be breached inadvertently or because of the seeming incompetence of a CCO. The sixth section was a fictitious scenario in which a fake retail account was discovered and what should have been done to rectify the situation.

The seventh section examined the SocGen scandal and whether Jérôme Kerviel was the sole culprit or whether SocGen formatted and distorted him. The facts indicated that both issues were involved in the scandal. The eighth section was a fictitious scenario where an individual with 30 years of experience working for a broker/dealer decided to become an investment adviser. The section talked about the advantages and disadvantages of hiring such an individual. The final section was a fictitious scenario in which three possible unauthorized trades occur. The questions raised in this scenario investigated the conditions under which a trade is truly unauthorized.

The cases and scenarios presented herein are issues that typically occur in a retail financial compliance situation. It should be remembered that cases and scenarios should not necessarily be taken at face value but researched to ensure that any decisions are fair and just. Retail financial compliance cases and scenarios are riddled with subtlety. Reasonable suspicion is needed to ensure that the appropriate facts are exposed. Accuracy is essential if only to safeguard the rights and fortunes of clients.

DONALD L. BURESH BIOGRAPHY

Donald L. Buresh earned his Ph.D. in engineering and technology management from Northcentral University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M. in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School) and an LL.M. in cybersecurity and privacy from Albany Law School, graduating summa cum laude. Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity, concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, quality management, management of non-

profits, negotiation skills, managerial ethics, and cybersecurity at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée and foil at a local fencing club. Dr. Buresh is a member of the Florida Bar.

LIST OF ABBREVIATIONS

Abbreviation	Description
AAR	Account Analysis Report
AML	Anti-Money Laundering
ATD	Automated Trading Desk Financial Services, LLC
AWC	Acceptance, Waiver, and Consent
BIS	Bureau of Industry and Security
BSA	Bank Secrecy Act of 1970
CCO	Chief Compliance Officer
CDD	Customer Due Diligence
CFPB	Consumer Financial Protection Bureau
CFR	Consumer Fraud Report
CGMI	Citigroup Global Markets, Inc.
Chardan	Chardan Capital Markets, LLC
CPR	Consumer Protection Rule
DTM	Division of Trading and Markets
EDD	Enhanced Due Diligence
ESG	Environmental, Social, Governance
FFI	Foreign Financial Institution
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
IAA	Invest Advisers Act of 1940
IBSG	CGMI Information Barriers Surveillance Group
ICBC	Industrial and Commercial Bank of China Financial Services, LLC
Jones	R. T. Jones Equity Management, Inc.
Laughton	Laughton Partners, LLC
LWL	Loans Watch List
MITM	Man-In-The-Middle Attack
MMA	Money Managed Account
MSSB	Morgan Stanley Smith Barney, LLC
MoneyGram	MoneyGram International, Inc.
NASD	National Association of Securities Dealers
NYSE	New York Stock Exchange
PEP	Politically Exposed Person
PERT	Program Evaluation Review Technique
PII	Personally Identifiable Information
REIT	Real Estate Investment Trust
RTL	Restricted Trading List
SAR	Suspicious Activity Report
SEA	Securities Exchange Act of 1934
SEC	Securities and Exchange Commission
Sheer	Sheer Partners, LLC
SocGen	Société Générale
SQL	Structured Query Language
TMS	Transaction Monitoring System
UBS	UBS Group AG
UBSFS	UBS Financial Services, Inc.
UBSS	UBS Securities, LLC
UIT	Unit Investment Trust
VFA	Voya Financial Advisers, Inc.

MISCELLANEOUS CONSIDERATIONS

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: I thank Leizza Buresh for her efforts in editing this paper and Peter Doro for his critical comments and insights. Any remaining issues are mine.

REFERENCES

1) Adam Hayes, Fiduciary Definition: Examples and Why They Are Important, Investopedia (Mar. 19, 2024), available at https://www.investopedia.com/terms/f/fiduciary.asp.
2) Adam Hayes, What Is a Broker/dealer (B-D), and How Does It Work?, Investopedia (Mar. 3, 2024), available at https://www.investopedia.com/terms/b/broker/dealer.asp.
3) Alyssa Pugh, Policies vs. Standards vs. Controls vs. Procedures, Tandem (Jan. 5, 2023), available at https://tandem.app/blog/policies-vs-standards-vs-controls-vs-procedures.
4) Bart Lenaerts-Bergmans, SQL Injection (SQLI): How to Protect Against SQL Injection Attacks, Crowd Strike (Oct. 10, 2022), available at https://www.crowdstrike.com/cybersecurity-101/sql-injection/.
5) BBC Staff, Rogue Trader Began Year in Profit, BBC News (Jan. 30, 2008), available at http://news.bbc.co.uk/1/hi/business/7218380.stm.
6) Beacon Pointe Staff, Does Your Advisor Use The Right Standard? Fiduciary vs. Suitability, Beacon Pointe (n.d.), available at https://beaconpointe.com/does-your-advisor-use-the-right-standard-fiduciary-vs-suitability/#:~:text=Established%20as%20part%20of%20the,them%20personally%20or%20their%20income.
7) Ben Martin, Nick Allen, Peter Allen, & Henry Samuel, Jerome Kerviel was 'honest, working class', The Telegraph (Jan. 28, 2008), available at https://web.archive.org/web/20080203164327/http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/26/nkerviel426.xml.
8) Book of Mormon, Alma 42:35
9) BRYAN A. GARDNER (ED. IN CHIEF), BLACK'S LAW DICTIONARY 658 (West Publishing Co. 8th ed. 1999).
10) CF Staff, Policies vs Standards vs Controls vs Procedures, Compliance Forge (n.d.), available at https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure#:~:text=Policies%20establish%20management's%20intent%3B,laws%2C%20regulations%20and%20frameworks)%3B.
11) CFPB Staff, What Is a Fiduciary, Consumer Financial Protection Bureau (Jun. 27, 2023), available at https://www.consumerfinance.gov/ask-cfpb/what-is-a-fiduciary-en-1769/#:~:text=A%20fiduciary%20is%20someone%20who,for%20their%20benefit%2C%20not%20yours.
12) Christine Sieb, Societe Generale missed 75 warnings on trader Kerviel, The Times (Feb. 21, 2008), available at https://www.thetimes.com/article/societe-generale-missed-75-warnings-on-trader-kerviel-xvzc27f09dn.
13) CNN Wire Staff, France's Biggest Rogue Trader to Serve 3-Year Prison Term, CNN News (Oct. 24, 2012), available at https://www.cnn.com/2012/10/24/world/europe/france-trader-case/index.html.
14) Courtney Comstock, Jerome Kerviel: "Jerome Kerviel had to be 'shot down.'", Business Insider (Nov. 16, 2010), available at https://www.businessinsider.com/the-greatest-interview-jerome-kerviel-has-ever-given-2010-11.
15) Courtney Comstock, Rogue Trader: Feel Bad for Me, I Was Just a Prostitute in the Banking Orgy, Business Insider (May 3, 2010), available at https://www.businessinsider.com/jerome-kerveil-feel-bad-for-me-i-was-just-a-prostitute-in-the-banking-orgy-2010-5.
16) Curio Staff, Broker Vs. Fiduciary: How Are They Different?, Curio Wealth (Jul. 18, 2022), available at https://curiowealth.com/broker-vs-fiduciary-how-are-they-different/#.
17) Cynthia Kroet, Rogue Trader Jérôme Kerviel Wins Unfair Dismissal Claim, Politico (Jun. 7, 2016), available at https://www.politico.eu/article/rogue-trader-jerome-kerviel-wins-unfair-dismissal-claim-societe-generale/.
18) DANIEL C. GOLDIE, & GORDON S. MURRAY, THE INVESTMENT ANSWER (Dan Goldie Investment Services 2010).
19) David Jolly, & Nicola Clark, Ex-Société Générale Trader's Huge Fine Is Cut to 1 Million Euros, The New York Times (Sep. 23, 2016), available at https://www.nytimes.com/2016/09/24/business/international/jerome-kerviel-societe-generale-fine.html.
20) Dodge v. Ford Motor Co., 204 Mich 459; 170 NW 668 (1919), available at https://casetext.com/case/dodge-v-ford-motor-co.

21) Due Diligence, Merriam-Webster Dictionary (n.d.), available at https://www.merriam-webster.com/dictionary/due%20diligence.
22) FINRA Staff, Communications with the Public: Regulatory Obligations and Related Considerations, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/rules-guidance/guidance/reports/2021-finras-examination-and-risk-monitoring-program/communications-with-public#:~:text=FINRA%20Rule%202210%20requires%2C%20among,"material%20fact%5Bs%5D%20or.
23) FINRA Staff, Letter of Acceptance, Waiver, and Consent, No. 2012034427001, Financial Industry Regulatory Authority (Dec. 17, 2018), available at https://www.finra.org/sites/default/files/UBS_AWC_121718.pdf.
24) FINRA Staff, Letter of Acceptance, Waiver, and Consent, No. 2014041196601, Financial Industry Regulatory Authority (Dec. 12, 2018), available at https://www.finra.org/sites/default/files/Morgan_Stanley_AWC_122618.pdf.
25) FINRA Staff, SEA Rule 15c3-3 and Related Interpretations, Financial Industry Regulatory Authority (Feb. 23, 2023), available at https://www.finra.org/rules-guidance/guidance/interpretations-financial-operational-rules/sea-rule-15c3-3-and-related-interpretations.
26) FINRA Staff, Segregation of Assets and Customer Protection: Regulatory Obligations and Related Considerations, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/rules-guidance/guidance/reports/2023-finras-examination-and-risk-monitoring-program/segregation-assets-customer-protection#:~:text=and%20Related%20Considerations,Regulatory%20Obligations,protect%20customer%20funds%20and%20securities.
27) FINRA Staff, Series 26 – Investment Company and Variable Contracts Products Principal Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series26.
28) FINRA Staff, Series 6 – Investment Company and Variable Contracts Products Representative Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series6.
29) FINRA Staff, Series 6 – Investment Company and Variable Contracts Products Representative Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series6.
30) FINRA Staff, Series 63 – Uniform Securities Agent State Law Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series63.
31) FINRA Staff, Series 7 – General Securities Representative Exam, Financial Industry Regulatory Authority (2024), available at https://www.finra.org/registration-exams-ce/qualification-exams/series7.
32) FINRA Staff, Watch for These 5 Behaviors by Your Registered Financial Professional, Financial Industry Regulatory Authority (Sep. 19, 2023), available at https://www.finra.org/investors/insights/watch-these-5-behaviors-your-financial-professional#:~:text=Using%20Personal%20Email%20or%20Text%20Messages&text=Required%20records%20include%20communications%20between,communication%20like%20email%20and%20texts..
33) Gabija Stankevičiūtė, What are the Five Pillars of AML Compliance?, iDenfy (Sep. 15, 2023), available at https://www.idenfy.com/blog/five-pillars-of-aml-compliance/.
34) Gordon Rayner and Peter Allen, Profile: Rogue Trader Jerome Kerviel, The Telegraph (Jan. 26, 2008), available at https://web.archive.org/web/20080128064429/http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2008/01/25/nsocgen325.xml.
35) Gregory White, Jerome Kerviel: I Faked Trades, Business Insider (Jun. 9, 2010), available at https://www.businessinsider.com/jerome-kerviel-i-faked-trades-2010-6.
36) Hannah Langworth, Rogue Traders: Jerome Kerviel, Trader Life (n.d.), available at https://traderlife.co.uk/series/rogue-traders/rogue-traders-jerome-kerviel/#:~:text=Though%20Kerviel%20would%20never%20become,career%20as%20an%20IT%20consultant.
37) Harvard College v. Amory, 26 Mass. 446 (1830), available at https://www.law.cornell.edu/wex/harvard_college_massachusetts_general_hospital_v._armory_(1830).
38) In the Matter of Chardan Capital Markets, LLC, Administrative Proceeding File No. 3-18486, U.S. Securities and Exchange Commission (May 16, 2018), available at https://www.sec.gov/litigation/admin/2018/34-83251.pdf.
39) In the Matter of Citigroup Global Markets, Inc., Administrative Proceeding File No. 3-16764, U.S. Securities and Exchange Commission (May 16, 2018), available https://www.sec.gov/litigation/admin/2015/34-75729.pdf.
40) In the Matter of Morgan Stanley Smith Barney LLC, Administrative Procedure File No. 3-19793 (May 20, 2020), available at https://www.sec.gov/enforcement/information-for-harmed-investors/morgan-stanley-smith-barney-llc.
41) In the Matter of R. T. Jones Equities Management, Inc., Administrative Procedure File No. 3-16827 (Sep. 22, 2015), available at https://www.sec.gov/news/press-release/2015-202.
42) In the Matter of Thomas E. Haider, Number 2014-08, U.S. Department of the Treasury: Financial Crimes Enforcement Network (Dec. 18, 2014), available at https://www.fincen.gov/sites/default/files/shared/Haider_Assessment.pdf.

43) In the Matter of Voay Financial Advisers, Inc., Administrative Procedure File No. 3-20183 (Dec. 21, 2020), available at https://www.sec.gov/files/litigation/admin/2020/34-90745.pdf.
44) Ina Grozeva, PERT Estimation: The Key to Successful Project Planning and Management, DevStride (n.d.), available at https://www.devstride.com/blog/pert-estimation-the-key-to-successful-project-planning-and-management#:~:text=The%20three%20estimates%20are%20then,accurate%20estimate%20for%20the%20task.
45) Infinite, Merrill Lynch Cut to 'Sell' at Goldman on Writedowns, Bloomberg News (Sep. 5, 2008), available at https://infiniteunknown.net/2008/09/06/merrill-lynch-cut-to-sell-at-goldman-on-writedowns/.
46) James Chen, Due Diligence, Investopedia (Jan. 18, 2024), available at https://www.investopedia.com/terms/d/duediligence.asp.
47) James Chen, Jerome Kerveil: A History and Work with Derivatives, Investopedia (Jum. 26, 2022), available at https://www.investopedia.com/terms/j/jerome-kerveil.asp.
48) James Chen, Prudent-Person Rule: What It Is, How It Works, Investopedia (Apr. 28, 2022), available at https://www.investopedia.com/terms/p/prudentmanrule.asp.
49) James Mackenzie, & Andrew Hurst, French Trader Kerviel Cooperating with Police, National Post (Jan. 26, 2008), available at https://archive.ph/20080128055324/http://www.nationalpost.com/news/story.html#selection-731.0-731.45.
50) Jean-Baptiste Vey, & Richard Lough, French Govt Indicates Will Reclaim SocGen Tax Deduction If Trader Wins Case, Reuters (Sep. 23, 2016), available at https://www.reuters.com/article/socgen-kerviel/french-govt-indicates-will-reclaim-socgen-tax-deduction-if-trader-wins-case-idUSL8N1BZ0OP/.
51) King James Version, Galatians 6:7.
52) Kinzer Yasar, Man-in-the-Middle Attack (MitM), Tech Target (Apr. 2022), available at https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM.
53) Mark Hendricks, A Guide to SEC Rule 15c3-3, Smart Asset (May 30, 2023), available at https://smartasset.com/investing/sec-rule-15c33.
54) Melissa Kluttz, Employee Due Diligence for Financial Services Industry, Sterling (Aug. 23, 2018), available at https://www.sterlingcheck.com/blog/2018/08/due-diligence-financial-services-industry-best-practices/.
55) Nicholas Economos, 5 Huge Differences Between a Fiduciary and a Broker (Part 1), Fiduciary Financial Partners (Apr. 11, 2022), available at https://www.fiduciaryfinancialpartners.com/blog/5-huge-differences-between-a-fiduciary-and-a-broker-part-1.
56) Robert Burns, To a Mouse, Poetry Foundation (n.d. [Nov. 1785]), available at https://www.poetryfoundation.org/poems/43816/to-a-mouse-56d222ab36e33.
57) SEC Staff, Merrill Lynch to Pay $415 Million for Misusing Customer Cash and Putting Customer Securities at Risk, U.S. Securities and Exchange Commission (Jun. 23, 2016), available at https://www.sec.gov/news/press-release/2016-128.
58) SEC Staff, What Is a Broker/Dealer?, U.S. Securities and Exchange Commission: Office of the Advocate for Small Business Capital Formation (n.d.), available at https://www.sec.gov/files/oasb-broker/dealer-building-block.pdf.
59) THE BIG SHORT (Adam McKay dir. 2015).
60) Thomspon Reuters Staff, What Is a Suspicious Activity Report?, Thompson Reuters Legal Solutions (2024), available at https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report#:~:text=A%20Suspicious%20Activity%20Report%20(SAR,of%20money%20laundering%20or%20fraud.
61) 15 U.S.C. § 80b-1 through 15 U.S.C. § 80b-21.
62) Wall Street: Money Never Sleeps – Plot, Internet Movie Data Base (IMDB.com) (n.d.), available at https://www.imdb.com/title/tt1027718/plotsummary/?ref_=tt_stry_pl.
63) Wonsover v. SEC, 205 F.3d 408(D.C. Cir. 2000), available at https://casetext.com/case/wonsover-v-securities-and-exchange-comm.