Right-Sized, Gated Ethics & Compliance Programs

Early-stage and small companies are not immune to ethics & compliance risks

By David Davidovic

Summary: Early-stage and small companies in all life-science sectors tend to unnecessarily delay foundational ethics and compliance initiatives, thinking they will be too costly and disruptive relative to where they are in terms of risk profile and resources. The reality is that they face many risks right from the start, and the most important risks can well be handled with a right-sized and gated program that takes into consideration the realities of a small company.

Despite the benefits that ethics and compliance programs offer, many early-stage and small companies resist or delay building one because they see this as a daunting task or as something they simply do not need at this point. Some companies have even stated that ‘they hire good people, with good values’; therefore, there is no need to add a compliance program to their burden. This approach, of course, ignores the fact that the life science industry is extremely complex, and there are multiple opportunities for failure – intentional or incidental.

The reality is that these companies have not encountered the same kind of legal, regulatory, and ethical scrutiny as their later-stage and larger peers have. The reasons for this lesser scrutiny are many and varied. For example, some entities are not at a stage (e.g., no commercial products) to encounter typical fraud-and-abuse concerns.

It is a valid point. However, as most of the industry’s compliance conversations, conferences, and articles highlight, regulators and prosecutors tend to focus on the risks associated with fraud and abuse, anti-kickback, off-label promotion, and a myriad of related areas. These risks typically involve commercially-marketed products that are reimbursed by federal and state health care programs, and prosecutions often result in significant financial and integrity-agreement settlements.
Others assert that it is too early to put in place potentially disruptive and burdensome internal policies and processes required by an ethics and compliance program. This assertion is especially prevalent among firms that are so focused on basic science and on making financial ends meet to support their early and costly scientific and product development efforts. When companies are literally years away from having an approved and sold product, their question about needing a program this early is a perfectly valid one.

However, the short answer to the question is “yes.” These companies do need a program, albeit smaller, focused, and gated. Early-stage and smaller companies face a multitude of ethics and compliance risks, and mitigation programs are important regardless of size or stage. Furthermore, it is never too early to start one and engrave the right culture, principles, habits, and structures into the company’s DNA. Having such an ethics and compliance culture is important for the company and its employees, scientific partners, vendors, regulators, potential acquirers, and investors, all of whom value and prefer companies with strong ethical practices.

In addition, ethical and compliance breaches are often more severe for small companies, threatening their very survival. Small companies are often ill-prepared for incidents of any magnitude that result in highly disruptive, costly, and crippling investigations and correction steps. Thus, they may be unable to recover fully from reputational or material losses.

**The Risk Footprint Is Larger Than You Think**

Contrary to “urban legend,” implementing an ethics and compliance program early in the company’s lifecycle does not need to be onerous, expensive, or disruptive. Instead, a simple but well-designed, right-sized, and gated program can help the company not only in terms of risk mitigation but also speed up and simplify early scientific, business, and funding efforts. Furthermore, an important and often unrecognized reality is that, even in small enterprises, company employees, contractors, and consultants make decisions every day that may have ethical and legal implications immediately or much later in the company’s life.

Even for small companies, the list of potential risk areas that can result in negative ethical, legal, financial, and reputational consequences (i.e., the risk map or risk registry) can be long (Table 1).

This article briefly examines each of the risk areas and discusses examples of steps that early-stage and small companies should consider.

### Asset Protection Including Intellectual Property & Data

After employees, intellectual property (“IP”) is arguably the most critical asset of a company regardless of size or development stage. IP production or enhancement begins on the company’s first day. For example, novel assets or scientific concepts are brought in and constitute the basis of the company’s formation and valuation from the beginning.

> “Trade secrets can be worth tens or hundreds of millions of dollars, and damage awards in trade secret litigation have been high; often, there is a lot at stake.”

In recent years, there have been numerous examples of the accidental loss or deliberate misappropriation of trade secrets. The types of trade secrets lost or misappropriated have included formulas, methods, processes, employee records, scientific data, and even physical materials. Only after these gaps are uncovered – sometimes years later –

---

**TABLE 1: Potential Risk Areas for Small Companies**

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Risk Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset protection including Intellectual Property and data</td>
<td>Reputation and credibility protection</td>
</tr>
<tr>
<td>External investor and scientific-community communications</td>
<td>Conflicts of Interest</td>
</tr>
<tr>
<td>Anti-competitive and antitrust risks</td>
<td>Harassment, discrimination, and whistleblowing</td>
</tr>
<tr>
<td>Obligations of scientific, research and technology partners</td>
<td>Privacy protection</td>
</tr>
<tr>
<td>Insider trading</td>
<td>Information security</td>
</tr>
<tr>
<td>Due Diligence</td>
<td>Executive accountability</td>
</tr>
</tbody>
</table>
is there a realization that more could have been done in the early and formative days.

There are some easy ways to safeguard trade secrets and minimize the risk of loss or misappropriation. Of course, companies actively and diligently file patents and effectively use publications to establish first use and prior art. Just as importantly, companies should restrict sensitive information to only those with a need to know or access it. Not everyone in the company needs access to every scrap of information. Companies should implement these efforts through a comprehensive set of policies and procedures governing information security, and incident response plans that guide where, how and to whom information is stored, accessed, and disseminated.

**External Investor and Scientific-Community Communications**

Communications to external investors and the scientific community are critical to the company’s quest for funding, partnerships, collaborations, and the credibility of its scientific story. Thus, these communications take a variety of forms, including, but not limited to, press releases, congress communications, regulatory filings, and business development presentations. There is also a wide range of applicable regulatory requirements depending on the form and the intended audience.\(^5\)

Therefore, the validity, credibility, and utility of these communications depend upon having robust discipline and well-managed controls around how that information gets developed, approved, disseminated, and protected. Furthermore, there have been several instances of premature or inappropriate external communications with impacts not only in the company itself but also on individual executives who have been convicted of wire fraud for creating and disseminating misleading information.\(^6\)

> **“When corporate executives provide false or fraudulent information about pharmaceutical trials, they jeopardize the public health and welfare.”**\(^7\)

Having clear external and scientific communication policies and procedures, including how decisions are made, who is permitted to communicate, and in what settings, are essential to mitigate these risks. These policies and procedures also need to address social media.

**Anti-Competitive and Antitrust risks**

Anti-competitive risk is one of the most pressing challenges facing small life-sciences companies. There is significant pressure on these companies to innovate and do so quickly, which is no easy task. However, the added pressure from other competitors, small and large, creates an additional dynamic that can create risk. Losing to the competition is a top reason why many startups fail.\(^8\) However, how companies behave with respect to one another, regardless of size, can be critical for survival and the competitive and antitrust risks are often subtle and difficult to manage.

For example, in life sciences, it is not unusual for Board of Directors members to sit on other company boards, creating potential “interlocking board” issues. While the various companies may not begin as competitors, they may become competitors as their research and development efforts progress.\(^9\)

An even riskier situation can occur when a company invites advisors based on their work with competitors, especially when there is an implicit expectation or hope that the company can learn about a competitor’s programs. Such situations are possibly unethical and could result in the advisor breaching their confidentiality provisions, potentially resulting in litigation.

Anti-competitive and antitrust risks can arise in many different scenarios. The most common scenarios include patent filings, intellectual property protection, customer and supplier agreements, mergers and acquisitions, pricing, and contracting. However, in the context of early-stage or even small companies, these risks often do not get the attention they deserve. But since President Biden’s Executive Order on protecting competition,\(^10\) the U.S. Federal Trade Commission (“FTC”) has become more active in healthcare antitrust matters.\(^11\) For example, one area of concern is the early detection, and presumably blockage, of “killer acquisitions” that companies can use to kill nascent potential rivals.\(^12\)

Given the complexities surrounding antitrust risks and the breadth of activities they can impact, there are no easy ways to mitigate the risks. Nevertheless, as with other risk areas, clear policies and procedures covering competitive intelligence gathering and intellectual property strategies are essential. In addition, periodic reviews of Board members and their outside interests can also help (see Conflicts of Interest section below). Finally,
information to trade in stocks or securities. As a result, it is an area that continues to be misunderstood or underestimated.

One reason for this situation is that many small companies are privately funded and do not issue stock. However, insider trading scenarios can arise when the company, its employees or the family members of employees trade in the stock of others, such as publicly-traded partners. For example, John Doe, an Employee works in business development and has knowledge of a deal that is about to be consummated between his company and another company “X.” John buys stock in company X anticipating a bump in their stock once the transaction is announced.

This scenario, and ones like it, have resulted in prosecutions with severe consequences to the individuals involved – including family members and acquaintances. In these cases, the companies’ reputations have been negatively impacted, not to mention the costly distraction of investigations, employee separations, and a general decline in trust.

Like antitrust risks, companies can mitigate the risk of insider trading through the establishment and clear communication of insider trading policies that apply not only to company officers but also to all employees, contractors, and consultants handling information that could be used to inform stock trades. Also, training with real-life, practical, and subtle examples can help crystallize the concepts of insider trading.

**Reputation and Credibility Protection**

A company’s short and long-term future depends on the reputation that it builds and maintains every single day. Unfortunately, the life sciences industry is characterized by complex business models filled with the potential for misunderstandings, mistakes, and lapses. We regularly see cases where individual or company reputations are destroyed, often without a chance of repair, based on lapses that could have been avoided. We have also seen
those lapses by individuals outside of their company’s activities can bring to the company potential losses of respect and reputation in the marketplace – or at least significant disruption.15

“It takes 20 years to build a good reputation and five minutes to demolish it.”16

A robust culture of ethics and compliance is central to protecting a company’s reputation and credibility. A well-written, easy-to-understand Code of Conduct and training that includes real-life cases and scenarios will help support that effort.

**Conflicts of Interest**

At a macro level, conflicts of interest (“COIs”) are intuitive and easy to comprehend. However, COIs can arise in multiple ways, including through direct economic relationships (e.g., ownership, employment) with others doing or seeking to do business with the company or more subtle relationships and dealings with competitors. COIs can also emerge through the provision of gifts, meals, entertainment, or the hiring or supervision of family members (i.e., perceived or actual nepotism). Recently, consulting companies such as McKinsey and Company have been the subject of damaging potential COIs caused by their advising on multiple sides of the same matter.17

As the McKinsey case demonstrates, COIs, not only can result in economic costs to the company and, by extension, shareholders, but they also can result in a loss of trust and confidence, damaging the company’s reputation and credibility. Once again, companies can mitigate potential COIs through the ethics and compliance program by establishing clear policies and procedures for preventing, identifying, handling, and correcting conflicts of interest. These processes include the availability of a hotline for reporting and a written procedure for the intake and handling of concerns brought up via any means. In addition, when a potential conflict is identified, it should be investigated and resolved.

Potential COIs are not entirely avoidable and can present themselves in many forms. Additionally, their resolutions can take several forms, including simple disclosure and mitigation measures such as oversight, but sometimes more severe measures are needed, such as recusals or even stopping any work on one or both conflicted sides.

**Harassment, Discrimination, and Whistleblowing**

Unfortunately, harassment and discrimination persist in companies of all sizes and at all stages of development. The same is true of whistleblowing.

There are common misconceptions about whistleblowers that border on outright skepticism.18 For example, there is the belief that most whistleblowers, especially False Claim Act whistleblowers, do so in the hope of receiving a reward or bounty.19

Another misconception is that whistleblower protections only apply to public companies. In 2012, Representative Lynn Woolsey (D-CA-6) introduced legislation to codify federal whistleblower protections for the private sector, state, and municipal employees who are retaliated or discriminated against by an employer for disclosing threats to public safety or violations of federal law.20 Under the proposed legislation, any whistleblower discharged or discriminated against by their employer could file a complaint with the U.S. Department of Labor or file suit in a U.S. district court.21 While the bill did not pass, whistleblowers are protected by a patchwork of laws and regulations that are not just limited to public companies.22

But setting aside any legal and reputational implications, including whistleblowers, of harassment and discrimination, these situations which create a hostile or uncomfortable work environment are unproductive and demotivating. Moreover, in extreme cases, the consequences of harassment and discrimination in the workplace can be devastating, especially when managers or senior leaders retaliate against employees who have raised concerns.

Therefore, companies must have a comprehensive approach to harassment and discrimination prevention and, when it occurs, rapid and effective handling. This approach needs to include a clear policy underscoring that harassment, discrimination, and retaliation, are not tolerated. It also needs to include an anonymous and confidential hotline that begins the process of investigating concerns. Finally, companies need to effectively and repeatedly train and educate employees on the policy and process for reporting concerns.

**Privacy Protection**

Life science companies should make employee, customer, and patient privacy a top priority, especially
in an increasingly digital world. In the face of exploding data needs and ever-advancing technologies, companies must make sure that they protect the data and information they collect, keep, and use. Likewise, regulators worldwide have grown increasingly concerned over privacy breaches instituting rigorous data handling and disclosure standards.

For very small companies, it can be difficult to invest in expensive resources like data encryption software and other advanced security measures. Thus, these companies are often less prepared to deal with privacy considerations. Furthermore, they may not understand the risks associated with data breaches or other privacy issues.

The consequences of privacy protection failures can be extensive, ranging from disruption to research and business activities to loss of trust and reputation and even legal actions, fines, and penalties.

“In addition to opening the door for regulators to initiate broader reviews into regulatory compliance, data breaches can result in significant liabilities beyond fines, such as liability arising out of contract disputes, product recalls, resignation of prominent executives, and plummeting stock prices.”

Like other risk areas, it is essential that companies have a clear data privacy policy that outlines what information may be collected and kept and for what purposes. Besides awareness training, companies need to map the data sources and identify the systems and the security controls housing and protecting that data. Finally, companies should identify someone within the organization, even if initially on an ad-hoc basis, who has the expertise and knowledge to create an effective privacy protection program as the company grows.

**Due Diligence**

Early-stage and small companies are in a constant state of due diligence in one form or another. As a result, they spend a lot of time and effort engaging in business development, mergers and acquisitions, financing and investment rounds, strategic partnerships, grants, sponsorships, and other arrangements.

It used to be the case that these types of transactions only focused on science, IP, and finances. However, that has changed. Now partners in these transactions frequently examine the companies’ ethics programs and practices because they are concerned about hidden risks that may taint the partnership at some point in their journey resulting in high legal costs, distractions, or worse.

There have been several cases of major acquisitions that soured once ethics and compliance lapses surfaced. For example, in one case, the acquiring company discovered, post-acquisition, that there were significant data integrity and manipulation issues that resulted in a disruptive and costly event including a drop in the acquiring company’s stock price.

Although the U.S. Department of Justice (“DOJ”) has made policy statements that ease the consequence of “inherited liability” in the case of a merger or acquisition, these are conditional and only provide partial relief, primarily in the area of corruption risk. However, the DOJ requires the acquiring company to conduct swift and effective due diligence after closing the deal. Therefore, the ideal situation for small and early-stage companies is to be “due-diligence ready” for any situation by building and demonstrating a program that prevents, detects and corrects risks (i.e., an ethics and compliance program). In this context, such a program can increase trust and speed and even add value to a transaction.

**Information Security**

Information is the lifeblood of all life science companies. It gets created, stored, transmitted, and used daily. It also is subject to misuse, neglect, or misappropriation, resulting in devastating information security breaches.

Cyberattacks and attempts to extract ransoms, infiltrations intended to steal secrets, or intrusions to sabotage operations frequently happen, even if not publicly disclosed. Some data and trade secret thefts have also occurred from within companies perpetrated by employees or contractors who had access to information beyond their needs relative to their work in the company resulting in some being charged with espionage.

The consequences of breaches and information loss include, but are not limited to, business and scientific disruption, disclosure of trade secrets, financial losses, regulatory actions, and loss of trust among partners. Therefore, an effective corporate ethics and compliance program must include a comprehensive risk assessment and preventive measures focused on physical or digital
information. It also needs to include mitigation steps, including not only education but also strict information access controls, technology barriers, early alarms, and a well-thought-out incident response plan.

**Executive Accountability**

Since 2017, the Justice Department has significantly increased its focus on individual accountability. In 2021, the DOJ announced further efforts to enhance its ability to hold individual corporate executives accountable. As a result, the government has secured several individual convictions and plea deals against current and former company executives.

Companies can no longer rely on just having an effective ethics and compliance program or assert the “rogue employee” theory when misconduct occurs. Instead, Boards of Directors and company leadership must take action when employee misconduct is uncovered or face the potential consequences for their inaction.

**What is a Company to Do?**

**Compliance is a journey, not a destination**

Perhaps the most essential take-away for companies embarking on developing an ethics and compliance program is to remember it is a mindset. Unfortunately, the ongoing bugle call to develop and implement “comprehensive and effective” programs is that it can paralyze a company’s leadership into inaction or avoidance. This paralysis stems partly from the mistaken belief that a company must do it all and do it perfectly.

However, this belief is fundamentally inconsistent with the tenets of the Sentencing Guidelines, which are couched in terms of “reasonableness” and minimizing the likelihood of wrongdoing. It also can create costly delays for companies until they feel ready and have resources to tackle “the big beast” — when small yet important steps will provide business value.

Setting the right tone, building the proper habits, and establishing credibility from the beginning are more impactful than a binder full of policies that sit on the shelf. Thus, building a solid foundation and approaching ethics and compliance as a right-sized and gated program allows for the correct outcomes while minimizing disruption and lowering overall cost and effort.

Foundation setting means making ethics and compliance a part of everyone’s responsibilities, not just the compliance officer or the compliance department. Compliance should be a standing agenda topic for the Board and the company’s Executive Team to ensure that key risk areas are identified and mitigated.

It also means developing the right written standards (e.g., a Code of Conduct and Employee Handbook) to guide employees in complex or challenging situations. It also means communicating expectations and keeping lines of communication open to learn about and address issues early on. Finally, it means a good early program is not a one-size-fits-all thing or a copy-and-paste exercise of another company’s program. Thus, it is never too early to start.

**References**

1 Mr. Davidovic is Founder of pathForward, a strategy advisory firm, and an industry expert having spent over 24 years with Merck & Co. and 8 with Genentech/Roche, in addition to his eight years advising companies across the life-sciences spectrum. He also is a member of the Editorial Board for the Policy and Medicine Compliance Update.

2 See, e.g., Seth Whitelaw and Manny Tzalakis, Ignorance is not Bliss — Why Hope and a “Fauth-Based” Approach to Compliance are Untenable; 7.9 POLICY & MEDICINE COMPLIANCE UPDATE 1 (2021).


4 See id. at 1-2.


7 See id. (quoting Ann Ravel, then-Deputy Attorney General for the DOJ’s Civil Division).


11 See, e.g., Robert Wilkey, Off-the-Air for Good – Pharma Bro Martin Shkreli Lose to the FTC, 8.2 POLICY & MEDICINE COMPLIANCE UPDATE 20 (2022); Gwendolyne A. Ball, Turning Up the Heat on Prescription Drug Pricing, 7.8 POLICY & MEDICINE COMPLIANCE UPDATE 8 (2021).

12 See Angus Liu, As FTC cracks down on pharma M&A, analyst sees potential chilling effect on large deals, FIERCEPHARMA (June 16, 2022), https://www.


16 Quote from Warren Buffet.

17 See Kirt Kraeuter, When It Rains, It Pours – McKinsey’s Reputation Takes Another Hit, 8.6 POLICY & MEDICINE COMPLIANCE UPDATE 17 (2022).


19 See id. at 5 (discussing whistleblower motivation).


21 See id. at §§ 103(b) and (c).


24 See Bianchi, supra n. 23.


27 See Memorandum from Brian A. Benckowski, Assistant Attorney Gen., U.S. Dep’t of Justice to All Criminal Division Personal, Selection of Monitors in Criminal Matters, 2 (Oct. 11, 2018); Memorandum from Lisa Monaco, Deputy Attorney Gen., U.S. Dep’t of Justice to All Component Heads and U.S. Attorneys, Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies, 4, fn 1 (Oct. 3, 2021) [hereinafter “Monaco Memorandum”].


The Shot Heard Around the Industry

As the Office of the Inspector General (“OIG”) for the Department of Health and Human Services has noted:

OIG is skeptical about the educational value of such programs. Our investigations have revealed that, often, HCPs receive generous compensation to speak at programs offered under circumstances that are not conducive to learning or to speak to audience members who have no legitimate reason to attend. Such cases strongly suggest that one purpose of the remuneration to the HCP speaker and attendees is to induce or reward referrals.³

Apart from the presence of alcohol, by the time the SFA was published the factors listed were an amalgamated restatement of the OIG’s previous positions that were indeed recognizable, at least to compliance professionals. However, to be fair, the SFA did not resolve all the potential issues surrounding these programs, and some have questioned whether the OIG might consider in-person speaking events at restaurants per se violations of the Anti-Kickback Statute (“AKS”), or will they examine the totality of the circumstances?⁴

Why are we still talking about speaker programs?

Fast-forward eighteen months to April 2022, when a panel of federal prosecutors took to the stage at Pharmaceutical Compliance Congress, bemoaning the industry’s continued practice of hosting speaker programs. Some on the panel seemed surprised and concerned that the industry had not immediately ceased these programs in the wake of the SFA, though there was some recognition that the quality of information exchange through in-person meetings is palpable when compared to virtual meetings.

Compliance officers were quick to address that these programs are inherently marketing events in nature and that many companies have sought, and through great efforts, to conduct effective and compliant programs and have implemented significant changes to their programs and corresponding compliance requirements over the years. For example, they highlighted their efforts to ensure compliance, including:

- Multi-modal monitoring that involves attendance by monitors who are true subject matter experts,
- Back-end records review program to keep a finger on the pulse of event-related communications, and
- Reviews of attendance sheets and expenses to ensure a complete understanding of the dynamics in play.

Thus, they held that in pre-pandemic times, most activities conducted by the field were fully vetted to identify and mitigate the common risks observed throughout the
industry. Also, through proper training and guidance, they noted organizations often could flag and mitigate risks before they became endemic within the organization. Still, despite notable efforts, some attendees remarked that speaker programs could sometimes come up short when scrutinized during compliance audits, CIA transaction reviews, investigations, and litigation.

What’s happening in the wild?

While Industry interactions with HCPs were significantly limited over the past two years, the full impact on the health care system and surrounding life sciences industries is only becoming evident as companies return to “normal.” Activities that were considered well-managed before the pandemic are creating a resurgence of old issues with the rise of less formal and controlled virtual detailing and speaker programs. Therefore, reliance on previously known and understood risk indicators and monitoring techniques may not fully capture potential compliance concerns emerging in today’s post-pandemic environment.

Overall, companies have adapted to the new environment caused by the pandemic with creativity, finding new and varied methods to reach their intended audiences. However some of these stay-in-market methods blur the lines between established business practices and compliance expectations. For example, using food delivery services to continue providing meals in conjunction with virtual speaker programs has been observed by some companies as an effective bridge between the virtual and in-person world. In contrast, others have shunned the practice in favor of death-by-1000 Zoom calls and Zoom calls only.

We observed the pivot to a nearly all-virtual world two years ago and, in the intervening period, have seen thinking and practices fluctuate as the pandemic era drags on. Because of this evolving landscape, communication is not always consistent or clearly understood, oversight is inherently more limited, and corrective actions can be more challenging to implement. Coincidentally (or not), field monitoring observations reveal some current behaviors reminiscent of behaviors considered on the fringe of industry trend lines leading into the pandemic. Below are several examples we have observed in conducting recent “live” field monitoring of speaker programs and other activities such as advisory boards. These examples are based on our observations across the country involving companies of all sizes across a broad spectrum of therapeutic areas.

Providing In-Office Meals

It seems that when it comes to feeding an HCP’s office, what is old is new again. Whether the program is held in a virtual or live setting, we have observed sales representatives providing food to staff who do not participate in the educational discussion despite some company policies directing a more focused program and aggregate meal cap (e.g., no more than five (5) meals at any one time in any one office). Nevertheless, it appears that feeding non-participants in some cases has become an expected practice in conjunction with office detailing. Although in most cases sales representatives are observed to be appropriately seeking time with physicians and other prescribers (e.g., nurse practitioners and physician assistants), the result is often feeding many to speak to a few.

This situation is not new, and the PhRMA Code addresses this practice, albeit with ambiguous language. The 2022 Code provides that companies may offer occasional and incidental meals to “healthcare professionals, as well as members of their staff attending presentations.” The key to providing meals to staff members turns on their participation. The Code states, “[o]ffering ‘grab-and-go’ meals is not appropriate.”

Appropriate Attendee Participation

Many company policies we have observed require that attendees participating in field educational promotional discussions, including speaker programs, not only practice in an appropriate specialty but also hold the appropriate credentials to attend the presentation. For example, while an organization may choose to invite ancillary staff to an event at an out-of-office setting, we have observed an increase in invitations being extended to non-prescribing office personnel as “seat fillers” to meet the company’s minimum confirmed attendance requirements.

In the early stages of the pandemic, we learned of cases where an HCP’s office provided a speaker program’s dial-in details to a competitor’s sales personnel. Although the PhRMA Code does not expressly address this situation, the Code provides that “[i]nteractions should be focused on informing health care professionals about products, providing scientific and educational information, and supporting medical education.”
However, ensuring that competitors do not have access to the program is a complex challenge facing companies, and it is unclear if this situation is still occurring.

**Speaker Interactions**

When engaging HCPs to be speakers, many companies we observe employ regimented nomination, qualification review, and selection processes. In these scenarios, speakers are selected based on their expertise and experience with treating a particular disease state and credible knowledge of product use in appropriate patient populations. Their capabilities are evaluated against objective criteria consistent with the PhRMA Code.\(^\text{14}\)

That said, even with the most rigorous consultant selection and field monitoring programs, we continue to observe speakers often sharing significant information from the pulpit, which may or may not be consistent with a company’s policies and expectations. For example, in delivering approved product messages and fielding appropriate question and answer sessions, speakers may use their speaking opportunities to subtly or not-so-subtly attempt to generate residual business through peer or patient referrals.

Of late, we have also observed a rise in informal clinical discussions in less formal engagements (e.g., journal clubs). The informal setting, combined with the lack of a traditional presentation slide deck, makes it more challenging to ensure that the discussion remains within regulatory boundaries. For example, speakers can discuss anecdotes and best practices tangentially related to the program’s topic and delve into nuances that may or may not be consistent with approved product messaging. They may thus derail the focus of the meeting in addition to raising potential compliance concerns.

**Patient Education Programs**

Patient education programs are a continuing challenge for the industry.\(^\text{15}\) Manufacturer-sponsored patient education programs provide an opportunity to reach out to the community and be of service in providing beneficial disease management information to patients and their caregivers, family, and friends. Although the stated objective is to support patients with quality disease education, based on our recent (and recurring) observations, these programs can present potential compliance concerns that are not always keyed into monitoring protocol.

These concerns include, but are not limited to:

- Patients attend programs with more than one caregiver or their entire family.
- Patients who take home multiple meals when the meals are arranged as a buffet or family-style.
- Patients receive token reminder items at the events, such as water bottles, calendars, backpacks, and other disease management items.
- Patients organize or plan attendance at future events amongst themselves at the end of programs. These situations often include sharing details of future programs hosted by the current sponsor and competitor manufacturers. Typically, patient attendees compare notes on food, location, and schedules resulting in ‘patient supper clubs’ inadvertently hosted by multiple unwitting manufacturers.
- Patients disclose sensitive healthcare information about themselves and others during discussions. These disclosures often are related to disease diagnosis or treatment but also include information about their experience with various medications (of the sponsoring manufacturer or others). These conversations sometimes go so far as to include patient-to-patient anecdotal accounts of product usage and dosing regimens that are off-label for the manufacturer’s product and that of another manufacturer. In some cases, the suggested product(s) referenced among patients are indicated for terminal disease management and carry significant side effect profiles.
- Patients disclose sensitive healthcare information about themselves and others during discussions. These disclosures often are related to disease diagnosis or treatment but also include information about their experience with various medications (of the sponsoring manufacturer or others). These conversations sometimes go so far as to include patient-to-patient anecdotal accounts of product usage and dosing regimens that are off-label for the manufacturer’s product and that of another manufacturer. In some cases, the suggested product(s) referenced among patients are indicated for terminal disease management and carry significant side effect profiles.
- Patient disclosures regarding in-depth information about clinical studies in which they have participated, or may currently be participating, related to a disease state topic or a new indication. The veracity of this information is often difficult to assess, as are patient use cases related to product labeling.

These scenarios create significant challenges for sales representatives and speakers alike. For example, while a company’s policy may require its representatives to interject and redirect patient-to-patient (mis)information exchange, the conversations are not always audible to everyone in the room, and company representatives may not have clear guidance on how to address these particular nuances. Additionally, speakers who are present as disease education consultants to a manufacturer may...
struggle with repeated requests for specific medical advice and may also encounter scenarios where unsanctioned patient-to-patient communications contain inaccuracies that may, ethically speaking, bear interjection and correction in the physician’s judgment.

While companies generally provide guidance that a physician or company representative direct a patient to consult with their own healthcare professional, the efforts to contain and focus patient education meetings abound. Furthermore, we have observed that while many companies provide some form of peer-to-peer patient education, some do not have dedicated policies and procedures governing patient education programs like those governing speaker programs. This situation creates areas of ambiguity and inconsistent approaches to managing disease education.

**Adverse Event Reporting**

Ensuring patient safety is an essential task for all pharmaceutical companies. Thus, it is crucial that product adverse event information gets to the company’s pharmacovigilance (i.e., drug safety or complaint handling) department for appropriate handling.

Sales team members naturally want to share information about their product benefits, including safety and effectiveness information, in a fair and balanced manner. However, there appears to be a lack of understanding on the part of some sales representatives about when a patient’s product experience needs to be shared with the pharmacovigilance team.

During our client monitoring work, we repeatedly encounter sales representatives who mistakenly believe that when a patient experiences a known product side effect, the information does not need to be reported to the pharmacovigilance team for evaluation as a possible adverse event. Although the experience may not be an adverse event, that is a decision for the experts (i.e., pharmacovigilance) and not the individual sales representative.

While it is impossible to ascertain why that belief persists in all cases, some field personnel have told us that previous reports of potential adverse events necessitating further follow-up with the HCP negatively impacted the HCP’s interest in prescribing the product to other patients. In some respects, this reasoning may be an “urban legend.” Nevertheless, it underscores the critical need for periodic refresher training on identifying and reporting product complaints and potential adverse event reports, and that safety is “Job 1.”

**Conclusions**

Over the long COVID winters, behaviors have changed, and old behaviors have resurfaced. Our experiences suggest that current field force activities, including those undertaken by medical science liaisons (“MSLs”), nurse educators, and HCP or patient spokespersons, present an opportunity to ramp up field monitoring and revisit field monitoring techniques to ensure that the company’s activities remain compliant as life returns to “normal.”

Doing so provides companies with a method to ensure that minor issues do not become systemic failures leading to possible enforcement actions. It also provides company leaders with a clearer picture of what is transpiring based on facts and data, rather than simply relying on hope and leaning on prior successes.

Early intervention is a strong antidote to address potential concerns – especially in light of the government’s sustained interest in field sales and marketing activities. Therefore, refreshing the strategy and executing on renewed and updated approach to field monitoring also provides compliance with an opportunity to engage in an open and candid dialogue about the realities field personnel encounter daily.

This refresher is especially valuable given the years of exclusive virtual communications that have permeated the pandemic era. And yes, we are still talking about speaker programs.

**References**

1. Ms. Gebrehiwiwet-Wilder, CCEP, is a Senior Associate with Epsilon Life Sciences. Ms. Norris, MPA, is a Managing Director with Epsilon Life Sciences and a member of the *Policy & Medicine Compliance Update* Editorial Board.
3. See U.S. Dep’t of Health and Human Services, Office of Inspector Gen’t, *Special Fraud Alert: Speaker Programs* 3 (Nov. 16, 2020) [hereinafter “SFA”].
Beginning in 2017, the U.S. Department of Justice (“DOJ”) significantly increased its focus on individual accountability and corporate compliance programs. However, these efforts achieved mixed results. On the one hand, the DOJ provided helpful guidance on what constituted effective corporate compliance programs. On the other hand, in life sciences, the Justice Department secured some individual convictions and plea deals against company executives, including some Chief Compliance Officers (“CCO”).

Since 2021, the White House has steadily, but relatively quietly, pushed for increased corporate accountability and adherence to the rule of law. For example, in July 2021, President Biden issued an Executive Order addressing various anti-competitive corporate behaviors. In addition, in October 2021, Deputy Attorney General Lisa Monaco issued a memorandum signaling a return to the Yates doctrine on individual accountability in the context of settlements and determining cooperation credit.

In its latest endeavor to hold corporations more accountable, the Justice Department recently announced plans to require CCO certifications as part of new corporate settlements. With this announcement, the pressure on CCOs, especially those compliance officers striving to resolve ongoing government enforcement actions, has increased.

A New Concept Emerges

The origin of the CCO certification is traceable to Deputy Attorney General Monaco’s remarks at the American Bar Association’s (“ABA”) 36th National Institute on White Collar Crime in October 2021. While primarily eclipsed by the announcement of the DOJ’s updated policy on prosecuting organizations, Monaco highlighted that “corporate culture matters” and “[a] corporate culture that fails to hold individuals accountable, or fails to invest in compliance – or worse, that thumbs its nose at compliance – leads to bad results.” She also indicated that DOJ would study “whether companies under terms of an NPA [Non-Prosecution Agreement] or DPA [Deferred Prosecution Agreement] take those obligations seriously enough ... [because the DOJ] has no tolerance for companies that take advantage of pre-trial diversion by going on to continue to commit crimes.” Although Monaco did not directly address the issue of CCO certifications, her comments about corporate culture and compliance resourcing foreshadowed what was to come.

DOJ’s Big Reveal

In March 2022, Assistant Attorney General Kenneth Polite addressed NYU Law’s Program on Corporate Compliance and Enforcement (“PCCE”). In his remarks,
Polite reiterated the three basic questions the DOJ asks when evaluating corporate compliance programs:

1. Is the corporate compliance program well designed?
2. Is the program adequately resourced and empowered to function effectively?
3. Is the program working in practice?

Polite added a fourth question to those three: Is the company demonstrating an ethical culture in practice?

Polite noted that CCOs, and their functions, need to have “true independence, authority, and stature within the company.” Therefore, he announced that:

In order to further empower Chief Compliance Officers, for all of our corporate resolutions (including guilty pleas, deferred prosecution agreements, and non-prosecution agreements), I have asked my team to consider requiring both the Chief Executive Officer and the Chief Compliance Officer to certify at the end of the term of the agreement that the company’s compliance program is reasonably designed and implemented to detect and prevent violations of the law (based on the nature of the legal violation that gave rise to the resolution, as relevant), and is functioning effectively. In certain resolutions, we will require additional certification language.

First Use

Shortly after Polite’s announcement, the Justice Department began implementing the new CCO certification requirement. In May 2022, DOJ announced a guilty plea and a $1.1 billion settlement with Glencore International A.G. to resolve allegations of foreign bribery and market manipulation. Glencore is a part of a Swiss commodity trading and mining firm.

According to the government, Glencore engaged in a decade-long scheme “to make and conceal corrupt payments and bribes” to foreign government officials. Additionally, Glencore admitted, “to engaging in a multi-year scheme to manipulate fuel oil prices at two of the busiest commercial shipping ports in the U.S.” Also, the government contended that Glencore had “inadequate anti-corruption controls and an inadequate compliance program and policies.”

As part of the settlement, Glencore established a centralized compliance function with a head of compliance, increased the staffing of the function, and invested in additional resources for real-time monitoring and training. Glencore also agreed to implement specific compliance provisions that track the DOJ’s guidance on evaluating corporate compliance programs. Overall, these provisions resemble a simplified version of the standard Corporate Integrity Agreement (“CIA”) provisions from the Department of Health and Human Services, Office of Inspector General (“HHS-OIG”).

The settlement also stipulates that 30 days before the expiration of the agreement (May 24, 2025), “the Chief Executive Officer and Head of Compliance ... will certify to the [DOJ] Fraud Section ... that the Defendant has met its obligations pursuant to this Agreement.” Those obligations include maintaining an effective compliance and ethics program, maintaining appropriate internal controls, cooperating with any ongoing government investigations, and self-reporting any evidence of bribery within the U.S.

The settlement agreement also specifies the form that the certification must take. The CEO and CCO must certify that Glencore has implemented an anti-corruption program that meets the specific requirements mandated by the settlement agreement. They also must certify that the compliance program “is reasonably designed to detect and prevent violations of the Foreign Corrupt Practices Act [“FCPA”] and other applicable anti-corruption laws throughout the Company’s operations.”

Concerns

Although Polite’s remarks were short on specifics, the idea of requiring CCO certifications has raised a host of concerns amongst legal and compliance professionals. Unfortunately, the Glencore settlement and the included certification language have done little to assuage those concerns.
**Expanded Liability**

The Justice Department has repeatedly stated that the new certifications are not “punitive” but rather are intended to empower compliance officers and to “ensure CCOs have ‘adequate visibility and access to information.’” However, many remain skeptical of DOJ’s motives, especially considering the Justice Department’s renewed emphasis on using the Yates doctrine to enforce individual accountability.

The Glencore certification explicitly clarifies that the Justice Department can hold a CCO liable for federal felony violations if the DOJ believes the certification contains false statements. Thus, the certification requirement can impose personal liability on CCOs not involved in misconduct or obstruction and shift “‘responsibility from business line personnel and management to the CCO.’”

Regardless of whether DOJ’s intent is punitive or empowerment, the new certification requirement places the CCO and DOJ in a heightened adversarial position. It also effectively undermines previous attempts by Mary Riordan, HHS-OIG Attorney, and others to convince industry compliance officers that the government views their work as essential and shares common objectives.

**Vague Standards**

Another concern is that the DOJ requires certification to a vague or ambiguous standard. For example, the Glencore certification requires that the CCO certify that “the compliance program is reasonably designed to detect and prevent violations” of the law (in this case, the FCPA). The concept of designing compliance programs to reasonably detect and prevent violations of the law is well-known within compliance circles. It is taken from the Federal Sentencing Guidelines for Organizations published in 1991. However, the elements of an effective compliance program were intended to apply to all organizations across industries. Thus the Commission explicitly recognized that any determination of whether an organization’s compliance program was effective required considering several factors, including “the size of the organization,” “the likelihood that certain offenses may occur because of the nature of its business,” and the organization’s prior history. Therefore, because of the inherent and necessary variability in compliance programs, the required reasonable design determination is not a simple binary choice. Instead, the determination is subject to different interpretations, and making the “wrong” determination could result in potential criminal liability.

In addition, the Glencore certification only speaks to reasonable “design.” Therefore, it is unclear whether an objectively well-designed program (e.g., one that follows the available guidance and leading practices) that fails to prevent a further criminal violation renders the certification false. I would argue that contrary to the strong language from Deputy Attorney General Monaco about recidivist organizations, it should not.

As the U.S. Sentencing Commission wrote, “[t]he hallmark of an effective [compliance] program ... is that the organization exercises due diligence in seeking to prevent and detect criminal conduct by its employees and other agents.” Thus, the Sentencing Commission’s statement acknowledged that the Commission never intended compliance programs as a guarantee that criminal conduct would not occur.

Furthermore, in *Safeo Insurance Co. of America v. Burr* and *Federal Communications Commission v. Fox Television Stations*, the Supreme Court determined a person cannot be liable for making reasonable statutory interpretations in the absence of authoritative guidance to know the interpretations were objectively unreasonable. Therefore, unless and until the DOJ clarifies the standard for CCO certifications, the Justice Department likely will find it challenging to hold CCOs accountable for alleged false certifications absent egregious circumstances.

**CCO as Superhero**

The Justice Department’s position and the Glencore certification also continue to perpetuate the myth of the CCO as a superhero capable of somehow forcing company employees to comply. For example, the Glencore certification requires the CCO to certify that upon reviewing reports made to the DOJ, the reports were “true, accurate, and complete.” The certification language contains no limitation or caveat, such as to the best of the CCO’s knowledge; it is just a binary choice.

Therefore, under this construction, a minor omission or even a numerical transposition could give rise to the DOJ contending the certification is false. While one would hope that the DOJ would not take such a draconian position, that is little comfort to the CCO facing the potential of substantial jail time.
Certification becomes even more complicated for a CCO, who oversees sizeable multi-national compliance operations. They must certify compliance with U.S. laws and regulations, as well as applicable international laws and regulations. Glencore, for example, operates in 35 countries and has 135,000 employees and contractors on the payroll. Given that Federal Sentencing Guidelines speak in terms of a single point of contact for compliance (e.g., a specific individual within an organization’s high-level personnel), this requirement is a daunting, if not impossible, task.

Regardless of the Justice Department’s viewpoint, CCOs are merely human, doing a difficult job often under criticism from their companies and external regulators. Unfortunately, both sets of stakeholders often expect perfection and not reasonableness as set out in the Sentencing Guidelines. This tendency is counterproductive and can lead CCOs to view everyone as “the enemy.”

**Conclusion**

There is an old tough-in-cheek compliance mantra that says, “We’re from the government, and we are here to help you.” While the current government position of empowering CCOs, increasing their visibility within organizations, and ensuring they have access to essential information is laudable, CCO certifications seem at best counter-intuitive and at worst counterproductive. As one law firm noted, currently, DOJ’s policies “put CCOs on a path toward potential individual liability without clearly indicating how they can ensure compliance with DOJ’s standards.”

Nevertheless, CCO certifications now seem destined to become additional boilerplate in government settlement agreements and, if history repeats, in OIG CIAs too. Therefore, it is incumbent that CCOs involved in settlement negotiations push for as little ambiguity as possible and begin planning now on how to make the required certifications less risky.

**References**

1. See U.S. Dep’t of Justice, Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (2017).


3. See U.S. Dep’t of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020).


9. See id.

10. See Polite Remarks, supra n. 7; see also U.S. Dep’t of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020).

11. Id.

12. Id.

13. See id.


15. Id.

16. Id.

17. Id.


19. Id. at 6, ¶ 7e.

20. See U.S. Dep’t of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020).

21. See Plea Agreement, supra n. 18 at Attachment C.

22. See id. at 9, ¶ 9.

23. See id. at 9, ¶ 9-10, ¶ 10; 11, ¶ 12; and 13, ¶ 13.

24. See id. at Attachment H.

25. See id. at Attachment H-1.

26. Id.

27. Id. at Attachment H-2.

28. See Polite Remarks, supra n. 7; see also Thomas Hanusik, et al., Empowering Chief Compliance Officers? Certifications are Now Required under DOJ Resolution Policy, CROWELL (June 24, 2022) (highlighting remarks by Lauren Kootman, Assistant Attorney General for Corporate Enforcement, Compliance, and Policy Unit of DOJ), https://www.crowell.com/NewsEvents/AlertsNewsletters/All/Empowering-Chief-Compliance-Officers-Certifications-are-Now-Required-under-DOJ-Resolution-Policy.


31. See Aaron Nicodemus, CCO liability framework seeks to acknowledge compliance support concerns, COMPLIANCE WEEK (Jan 12, 2022), https://www.complianceweek.com/regulatory-enforcement/ccoiability-framework-seeks-to-acknowledge-compliance-support-concerns/31239.article.

32. See Plea Agreement, supra n. 18 at H-1 (emphasis added).


34. See id.

Challenging Objective Reasonableness for FCA Cases

Senator Grassley Files an Amicus Brief with the U.S. Supreme Court

By Robert N. Wilkey, Esq., Senior Staff Writer

Summary: The ongoing SuperValu case involves crucial questions about the breadth of false claims liability for defendants making objectively reasonable interpretations of the statute without definitive guidance. The case is now before the U.S. Supreme Court, which recently received the perspective of Senator Charles Grassley, a principal sponsor of the 1986 False Claims Act amendments. Thus, Grassley is uniquely positioned to guide the Court on what Congress intended when it enacted its three-part knowledge criteria.

Over the past two years, when it comes to the Federal False Claims Act (“FCA”), Senator Charles Grassley (R-Iowa) has been busy. In November 2021, he was the primary sponsor of a bill to amend the FCA.1 The bill purports to help relators by reducing the legal hurdles relators face when bringing false claims cases and decreases the DOJ’s ability to move to dismiss certain qui tam cases unilaterally. It also provides some protections to government agencies with a procedure to limit discovery costs that qui tam parties can impose.

In May 2022, he filed an amicus brief supporting a Petition for Writ of Certiorari before the U.S. Supreme Court challenging a recent opinion by the U.S. Seventh Circuit Court of Appeals.2 Grassley argues that the Seventh Circuit “badly distorted Congress’s plain language in reaching a result that opens a gaping hole in the government’s primary fraud-fighting tool,” the FCA.3

State of Mind

Unlike the Federal Food, Drug, and Cosmetic Act, the FCA is not a strict liability statute. Instead, the FCA requires a showing that a person “knowingly” creates or uses a false record or statement material to a government obligation or “knowingly” conceals, avoids, or decreases their obligation to the government.4 Furthermore, the statute defines “knowingly” as having actual knowledge of the information, acting in deliberate ignorance of the truth or falsity of the information, or acting in reckless disregard of the information’s truth or falsity.5 However, the FCA requires “no specific intent to defraud” to impose liability.6 Thus, a defendant must have the requisite state of mind or scienter in legal jargon for an act to violate the FCA.

Prior Supreme Court Precedent

In 2007, in a case involving the Fair Credit Reporting Act (“FCRA”), the U.S. Supreme Court held that a defendant does not act with reckless disregard if the defendant made a reasonable interpretation of the statute and there is insufficient authoritative guidance for the defendant to know that the interpretation was unreasonable.7 Thus, the Supreme Court defined recklessness as “‘conductive violating an objective standard: action entailing ‘an unreasonably high risk of harm that is either known or so obvious that it should be known.’”8 Therefore, the proper test is (1) whether the defendant’s interpretation is objectively reasonable and, if so, (2) was there authoritative guidance to warn the defendant away from that interpretation.9

The SuperValu Case in a Nutshell

The Allegations

SuperValu is a conglomerate that owns or operates approximately 2,500 retail grocery stores and over 800 pharmacies in 25 states.10 Specifically, the states include California, Delaware, Idaho, Illinois, Indiana, Iowa, Maine, Maryland, Massachusetts, Minnesota, Missouri, Montana, Nevada, New Hampshire, New Jersey, North Carolina, Oregon, Pennsylvania, Rhode Island, Utah, Vermont, Virginia, Washington, Wisconsin, and Wyoming.11

In 2011, two pharmacists, Tracy Schutte and Michael Yarberry, filed a qui tam lawsuit alleging that SuperValu Inc. and its co-defendant pharmacies “knowingly failed to report accurate usual and customary prescription drug pricing [U&C pricing] to government healthcare programs.”12 Thus, the pharmacists asserted that SuperValu and its affiliates, including SuperValu Pharmacies, Albertsons, and Acme, submitted false claims for government reimbursement.13

References

3. See Plea Agreement, supra n. 18 at H-2.
4. See Cassin, supra n. 29.
6. See Sidley Austin, supra n. 29.
According to the pharmacists, SuperValu centrally controls the billing, marketing, and price matching for the pharmacies under its control. Thus, in late 2006, SuperValu allegedly implemented a price matching program under which the SuperValu-controlled pharmacies matched specific competitors’ prices for generic drugs. Consequently, these price matches, not cash prices, became the U&C prices that SuperValu disclosed to the government.

The pharmacists supported their claims with “computer printouts of customer transactions from the Defendants’ centralized claims processing system which show the low prices charged the general public and the inflated prices charged the government health programs for the same drugs.” Thus, by persisting in using the cash prices as their U&C pricing, SuperValu submitted false claims to federal healthcare programs and obtained higher reimbursements.

The Central Issue

The primary dispute was whether SuperValu was “required to account for discount price matching programs when they report their usual and customary prices [where] pharmacies will—upon customer request—match a lower price offered by a competing pharmacy.” In 2016, the Seventh Circuit addressed the issue of discounted cash prices for purposes of U&C pricing calculations. In Garbe, the Court determined that:

Because Kmart offered the terms of its “discount programs” to the general public and made them the lowest prices for which its drugs were widely and consistently available, the Kmart “discount” prices at issue represented the “usual and customary” charges for the drugs.

Therefore, based upon this earlier ruling, the Relators contended SuperValu was required to report these prices and, by failing to do so, defrauded multiple government healthcare programs by falsely inflating reimbursements.

SuperValu responded by asserting that the Relators failed to demonstrate any fraud under the FCA because they failed to allege facts supporting the elements of “falsity,” “knowledge,” and “materiality.” Thus, SuperValu contended that they were entitled to summary judgment. However, the District Court disagreed.

Lack of Clear Guidance

SuperValu also argued there was no clear guidance on whether it was required to report specific discounts. In support of their assertion, SuperValu noted that “the pharmacy benefit managers [“PBMs”] who processed their prescription records did not consider the individualized price matching to have altered the usual and customary prices they submitted.” Therefore, SuperValu contended that the PBMs and state Medicaid programs were well aware of the situation, and after a three-year investigation, the government declined to intervene in the case.

Applying the U.S. Supreme Court’s Safeco standard, the District Court determined that “SuperValu’s understanding of U&C price, while incorrect, was objectively reasonable at the time.” Furthermore, “it was unclear that SuperValu’s program fell within the U&C definition [and] there was no authoritative guidance to warn SuperValu away from its interpretation of U&C price.”

Strike Two

Having failed at the District Court, the Relators appealed to the Seventh Circuit. The Court framed the issues as whether “Safeco applies to the FCA’s scienter standard and, if so, to what extent” and “whether the district court properly granted summary judgment for SuperValu on the scienter prong of the FCA claim.” Once more, the whistleblowers’ case failed.

Beginning with the FCA statute, Circuit Judge St. Eve noted that the FCA imposes two basic requirements: falsity and knowledge (scienter). Knowledge is defined explicitly by the statute and includes:

1. Actual knowledge,
2. Acting in deliberate ignorance of the truth or falsity of the information, or
3. Acting in reckless disregard of the truth or falsity of the information.

In addition, the Supreme Court interpreted the statute as requiring that the false claims must be material to the government’s payment decisions. Therefore, “a party who submits a false claim to the government is on the hook for FCA liability only if it acted knowingly.”
However, the Court viewed the FCA’s statutory definition of knowledge as a “range of ... levels,” and the statute does not “further define those terms.” Therefore, the Court turned to the Safeco decision for further guidance, even though the case involved the FCRA and not the FCA.

Judge St. Eve noted that Safeco defines the FCRA’s common-law scienter requirement as requiring proof that the defendants “acted ‘willfully.’” The Court also noted that acting willfully applied to both “knowing” and “reckless disregard.” According to the Court, Safeco’s analysis is relevant to FCA cases because there is “no statutory indicia that Congress intended the familiar, common law terms used in [the FCA] to differ from their common-law meaning.” Judge St. Eves also noted that this application follows the Supreme Court’s guidance in Escobar. Finally, the Court noted that four other circuits have applied the Safeco standards to “the FCA’s scienter prong.”

Having determined that Safeco’s knowledge interpretation applies to FCA cases, the Court proceeded to apply the Supreme Court’s two-part inquiry where plaintiffs allege defendants acted in reckless disregard of the truth or falsity of the information submitted for government payment. The first part involves determining whether the defendant’s statutory interpretation was “objectively reasonable” even if erroneous. If it was reasonable, the second inquiry is whether any “authoritative guidance” existed, warning the defendant that its interpretation was faulty. In this case, the Court found that:

Because SuperValu had an objectively reasonable understanding of the regulatory definition of U&C price and no authoritative guidance placed it on notice of its error, the Relators have not shown that SuperValu acted knowingly.

Thus, the Court of Appeals affirmed the District Court’s opinion.

In Dissent

Circuit Court Judge Hamilton, however, filed a vigorous dissent about the “majority’s Safeco tangent.” Specifically, he objected to the majority’s approach that departed from “focusing on the language of the False Claims Act itself and its origins in the common law of fraud and responses to crabbed judicial interpretations.”

Citing various reasons that the majority erred, Judge Hamilton noted that reliance on Safeco is “neither necessary for fitting for the False Claims Act,” and the opinion “effectively nullifies two-thirds of the statutory definition of “knowing.” Therefore, “the majority’s approach actually leaves the False Claims Act definition of knowledge narrower than when the 1986 amendment was passed.” Thus, he concluded, “With respect, I believe that both Congress and the Supreme Court will be surprised by this decision.”

Grassley’s Amicus Brief

The case is now on appeal to the U.S. Supreme Court, and Judge Hamilton’s prognostication about surprise seems correct. Apparently, it was such a surprise that Senator Grassley chose to file an amicus brief with the Supreme Court arguing that:

The majority below, however, ignored this text and structure. [ ] It held that a defendant who correctly knows an act is unlawful is immunized from FCA liability if its lawyer, years later, can cook up an interpretation of the law under which the act was arguably permissible— even if that interpretation is wrong and the defendant did not have that interpretation at the time. That test makes a hash of the law of fraud, which focuses on what a defendant understood at the time it undertook a fraudulent act.

The focus of Grassley’s brief is that the Seventh Circuit essentially rewrote the statute by collapsing “the three separate routes to liability that Congress laid out into one.” Furthermore, he asserts that the objective reasonableness standard “puts on the government a nearly impossible burden to anticipate and warn future fraudsters from every colorable misinterpretation of the law.”

To support his position, Grassley notes that Congress created three different scienter requirements with the “unmistakable goal ... to assure that the FCA would be applied liberally and expansively as the government’s primary tool to combat fraud.” Moreover, Congress intended these requirements to function independently, so the government only needed to establish “any one of them.” However, “[n]otwithstanding this painstaking textual clarity, the SuperValu majority ignored Congress’s formulation and effectively rewrote the statute to achieve its result.”

In essence, Grassley asserts that the lower court engaged in judicial activism and impermissible overreach by creating a “new scienter test from whole cloth.”
Beyond judicial activism and overreach, Grassley contends that the Seventh Circuit’s ruling effectively immunizes defendants from FCA liability without “definitive guidance” from the government that their actions were wrong. Thus, the lower court’s ruling “places the burden on the government to anticipate every possible fraud” requiring the government to “endlessly issue ‘definitive guidance’ to proscribe it.”

It also raises the difficulty of determining what constitutes “definitive guidance.” As Grassley outlines, in this case, the Seventh Circuit rejected “abundant compelling contract language” and federal and state regulations supporting liability because they did not come from the judiciary or the “relevant agency.” Likewise, the Court also rejected guidance from the Centers for Medicare and Medicaid Services (“CMS”) because it lacked the necessary high-level specificity. Thus, Grassley argues the decision provides “a robust liability shield for plainly culpable defendants.”

Finally, Grassley asserts that placing such a burden on the government is inappropriate because the FCA “was conceived in response to a crisis, the Civil War.” At first blush, this argument seems disingenuous and unpersuasive. However, Grassley ground this assertion in a modern context. During the COVID-19 pandemic, the government expended trillions of dollars to support the American public. However, because of the situation’s urgency, there was no time to issue “definitive guidance.” In appropriating COVID-19 relief funds, Congress “did not envision that the courts would impose this onerous requirement as a prerequisite to recovering money stolen by fully culpable defendants.” Instead, Congress intended:

> Those accepting government funds ... to "turn square corners," not hope the government will fail to anticipate their deceptive scheming.  

**Conclusion**

The *SuperValu* case is the latest installment in the ongoing legal debate surrounding whether a defendant can violate an ambiguous statute or regulation without clear guidance on interpreting it. Beginning with the *Safeco* decision in 2007, the U.S. Supreme Court reinforced this notion in its 2012 *Fox Television* opinion. Thus, the Supreme Court has signaled a growing reluctance to allow enforcement agencies to use prosecutions to avoid the work of providing meaningful guidance. Furthermore, legislative intent is essential when trying to tease out statutory meaning. Since Grassley was involved with the 1986 FCA amendments, and subsequent legislative attempts to amend the statute, the Supreme Court should carefully consider its view on what Congress intended. The Court can rarely hear directly from a first-party source. Instead, the Court must often rely on the Congressional Record or other third-party sources to divine Congressional intent.

Although the outcome of this case is far from certain, we believe it is an important case for the life science community and its compliance professionals since FCA liability represents a significant risk to the industry.

**References**

3. See id. at 23.
8. See id. at 68 (citation omitted).
9. See id. at 69-70.
11. Id.
13. See id.
14. See Dismissal Opinion, supra n. 10 at 3.
15. Id.
16. Id. at 4.
17. See id. at 3-4.
18. See PubKGroup, supra n. 12.
20. Id. at 645.
21. See PubKGroup, supra n. 12.
22. See Dismissal Opinion, supra n. 10 at 8-12.
24. Id.
25. See PubKGroup, supra n. 12.
26. See id.
27. See 7th Circuit Opinion, supra n. 23 at 462.
28. See id.
29. Id. at 463.
30. Id. at 459.
31. Id. at 463 (citing 31 U.S.C. § 3729(a)(1)(A)).
32. Id. (citing 31 U.S.C. § 3729(b)(1)(A)).
For decades, genetic testing has dangled the prospects of individually tailored health care treatments and improved outcomes. For example, in the 1990s, Human Genome Sciences (“HGS”) was founded by William Haseltine to “speed up biological discovery [by] a hundredfold.” Although acquired by GlaxoSmithKline in 2012, the promise never materialized. Nevertheless, despite its apparent failure as a standard drug development tool, “genetic testing has become a powerful new tool for improving health care and controlling health care costs.” Beyond the direct-to-consumer genetic testing pioneered by 23andMe and others, the government recognizes that genetic testing can be a critical diagnostic tool, in part accounting for Medicare genetic testing expenditures increasing more than 530% from 2016 to 2019 ($1.3 billion versus $7 billion).

However, in addition to privacy concerns, the billions of dollars spent on genetic testing provide ample incentives for fraud and abuse. Thus, reimbursement claims are only valid for “reasonable and medically necessary” tests. A recent trio of cases highlights the U.S. Department of Justice’s (“DOJ”) ongoing efforts to address genetic testing fraud.

**Watching Closely**

For the past several years, the DOJ has closely watched the genetic testing industry because of concerns about the lack of regulatory compliance. In September 2019, the Justice Department announced the takedown of one of the largest health care schemes involving “fraudulent genetic cancer testing [that] resulted in charges in five federal districts against 35 defendants associated with dozens of telemedicine companies and cancer genetic testing laboratories.” According to the DOJ, the federal investigation targeted an alleged scheme “involving the payment of illegal kickbacks and bribes by CGx [cancer genomics] laboratories in exchange for the referral of Medicare beneficiaries by medical professionals working with fraudulent telemedicine companies for expensive cancer genetic tests that were medically unnecessary.”

According to the Justice Department, there were several issues with the testing. These issues included:

- Failing to provide test results to the individual beneficiaries (i.e., patients),
- Providing test results that were “worthless” to the patients’ physicians, and
- Using a telemarketing network that required patients to pay doctors to prescribe the tests, either without actual patient interactions or upon brief conversations with patients they had never met or seen.

In early 2020, the America Bar Association (“ABA”) highlighted the DOJ’s renewed scrutiny of the genetic testing industry.
testing industry. The ABA noted that pharmacogenetic or pharmacogenomic (“PGx”) tests are “a major growth area in the genetic testing industry where concerns over fraudulent conduct have arisen.” Based on those concerns, the report noted that “the federal government has launched over 300 investigations into alleged fraud in the genetic testing industry, many of which are almost certainly ongoing.” Furthermore, while “genetic testing has promising medical uses [and] its prospects are broad, with potential applications across the medical spectrum, its potential remains largely unrealized at this juncture. Consequently, there is “limited [scientific] evidence supporting genetic testing to date” and therefore, “Medicare has generally recognized that PGx and other genetic tests are medically necessary in only a very narrow set of cases” and that “a test must still be reasonable and medically necessary.”

Reviewing the genetic testing cases to date, the ABA highlighted several recurring fraud schemes. These schemes included:

- Providing remuneration or consulting fees to physicians for advocating on behalf of the genetic testing industry,
- Using medical service organizations (“MSOs”) to serve as third-party payment processors for genetic testing services,
- Creating pass-through billing arrangements where “a physician purchases a test from the lab and is then entitled to bill payers for the test,” and
- Making commission-based payments to independent marketers for referrals.

The recent case involving BluWave Healthcare Consultants, Inc., Health Diagnostic Laboratory, Inc., Singulex, Inc., and Berkley Heartlab, Inc., is emblematic of the fraud schemes identified by the ABA. According to the Government, BlueWave allegedly promoted the services of HDL and Singulex to physicians using “lucrative offers to pay sham ‘processing fees’ to referring physicians.” However, BlueWave, HDL, and Singulex contended these “process and handling fees” (“P&H fees”) were appropriate compensation to cover physician costs involved in drawing, preserving, and shipping the blood samples to the labs. For example, HDL paid physicians a $3 “draw fee” and $17 for storage and shipping.

Acting essentially as a sales representative for Exceltox, Rehfuss worked to “convince senior citizens to submit to the genetic testing [by using] fear-based tactics during the presentations, including suggesting the senior citizens would be vulnerable to conditions such as heart attacks, stroke, cancer or even suicide if they did not undergo genetic testing.”

To get the tests authorized, Rehfuss “advertised on Craigslist to recruit health care providers who Rehfuss and others paid thousands of dollars per month to sign their names to requisition forms authorizing testing for patients they never examined or had any interaction with.” In fact, Rehfuss and his conspirators “established email accounts,
phone numbers, and “office manager” names for the requisition forms that made it seem as though the health care providers were treating the patients and would be evaluating their test results.” Exceltox, in turn, submitted claims for payment to Medicare for the contractor’s genetic tests that were performed without any proper physician medical oversight or approval.

In mid-December 2020, Exceltox agreed to settle with the Justice Department for $357,584 to resolve its FCA-related liabilities. However, Exceltox did not admit to any liability.

Before the Exceltox settlement, Rehfuss was indicted on one count of conspiracy to commit healthcare fraud and one count of conspiracy to access individually identifiable health information and paying kickbacks wrongfully. He pled guilty to a single consolidated conspiracy count and was sentenced to 50 months in prison. However, Rehfuss challenged enhancements to his sentence under the Federal Sentencing Guidelines for his leadership role, using a charitable organization to commit fraud, and targeting senior citizens. The Third Circuit Court of Appeals rejected his appeal.

**UC-San Diego Health**

In January 2022, the Justice Department announced a settlement with UC-San Diego Health (“UCSD”) to resolve allegations that it ordered medically unnecessary genetic testing violating the FCA. According to the government, for almost four years, UCSD physicians ordered and submitted referrals for these tests performed by three laboratories owned by the Tennessee company, CQuentia. These orders and referrals resulted in the submission of false claims to Medicare.

CQuentia was the subject of a prior FCA action alleging that “the company made bogus claims to consumers that its genomic tests could protect them from adverse drug reactions.” At this point, CQuentia apparently is no longer in business.

UCSD agreed to pay $2.98 million for its part in the scheme with no admission of liability. However, the settlement did not release any liability for the individuals. As Acting Assistant Attorney General Brian Boynton said, “Hospitals are the gatekeepers for medical care and are expected to ensure that all services performed at their direction, including genetic tests, are medically appropriate [and] the department will continue to pursue those who undermine the integrity of federal health care programs and waste taxpayer dollars.”

**Physician Partners of America**

In April 2022, the Justice Department announced another genetic testing settlement, this time with Physician Partners of America, LLC (“PPOA”), the company’s founder and owner, Dr. Rodolfo Gari, and its former chief medical officer, Dr. Abraham Rivera. PPOA, located in Tampa, Florida, is a practice management group. PPOA managed Florida Pain Relief Group, Texas Pain Relief Group, and indirectly owned Medical Tox Labs, Medical DNA Labs, and Physician Partners of America CRNA Operations, LLC.

According to the government, PPOA submitted false claims to federal healthcare programs “for unnecessary medical testing and services [and] paying unlawful remuneration to its physician employees.” The medical testing involved both urine drug testing and genetic testing. The government also contended that PPOA falsely certified it was not engaged in “illegal activity” when it secured a Paycheck Protection Program (“PPP”) loan in April 2020.

In the case of genetic testing, the Justice Department alleged that “PPOA required patients to submit to genetic and psychological testing before the patients were seen by physicians, without making any determination as to whether the testing was reasonable and necessary, and then billed federal healthcare programs for the tests.”

Once again, in exchange for paying $24.5 million to resolve this matter, PPOA admitted no liability. The settlement also resolved four outstanding qui tam lawsuits filed between 2018 and 2020. In addition, PPOA agreed to a five-year Corporate Integrity Agreement (“CIA”). As the DOJ explained, “billing federal healthcare programs for services that providers know are unnecessary or unreasonable undermines the quality of care that patients receive and increases the costs of these taxpayer-funded programs [and] the department is committed to ensuring that healthcare providers base their treatment decisions on their patients’ needs rather than their own financial interests.”

**Conclusions**

These three recent cases emphasize the ongoing efforts by the Justice Department to route out fraud involving genetic testing, as the ABA predicted back in 2020.
Unfortunately, they also highlight the elaborate and complex schemes being concocted by laboratories, sales representatives, health care providers, and other third parties within the genetic testing industry.

These enforcement actions demonstrate that the DOJ’s regulatory focus regarding medically unnecessary genetic testing is broad in scope and is not limited to one specific type of participant. Instead, the Justice Department has demonstrated a willingness to apply liability equally to all participants, including the manufacturers, laboratories, hospitals, physicians, and sales representatives.

These actions also demonstrate that any genetic testing that is not approved or determined medically necessary by a legitimate healthcare professional can become a per se FCA violation if reimbursed by federal healthcare programs (e.g., Medicare). There are emerging standards as to what constitutes “medically necessary.”

As one group of physicians has opined, “the individual’s medical record must contain documentation that justifies the medical necessity for a particular genetic testing service: medical history, physical examination, and results of pertinent diagnostic tests or procedures.” Thus, the general criteria for medical necessity include:

- The individual displays clinical features or is at direct risk of inheriting the mutation in question due to its identification in a family member (pre-symptomatic),
- The results of genetic testing are being used to inform clinical interventions, detect diseases when treatments are available, manage symptoms, or slow the progression of established disease,
- A definitive diagnosis remains uncertain after the completion of traditional diagnostic studies, physical examination, pedigree analysis, genetic counseling, and
- Disease-specific criteria are met.65

The Clinical Laboratory Improvement Amendments (“CLIA”) program and the FDA have sought to mandate that laboratories and testing facilities “meet the CLIA standards for quality, accuracy, and reliability of testing, as well as personnel requirements for high-complexity testing.”54

Several state agencies in California and New York have adopted more stringent criteria in addition to the CLIA requirements.55 For instance, “in California, all laboratories need to be licensed by the state and meet federal CLIA requirements, and tests cannot be offered to individuals without a physician’s order.”56 Also, “California state law addresses genetic testing to ensure that test results are accurate and valid and offered only with sufficient medical oversight to avoid unnecessary harm.”57

Finally, it seems apparent that given the increased use and importance of genetic testing in health care, the industry is likely to become more regulated by the federal and state governments and result in additional DOJ enforcement actions. As a result, within the health-care industry, there is a concerted effort:

by many other groups [to] assist in oversight, including payers, professional societies and industry organizations, private-sector accreditation bodies, and individual advocacy groups [and] this oversight has been achieved by developing evidence-based clinical and laboratory practice guidelines, establishing standards, and accrediting clinical laboratories.68

The net result is that compliance professionals working in this space must remain vigilant as these developments progress.

References

3. See Allen, supra n. 1.
9. Id.
10. Id.
11. See Owens, supra n. 7.
12. Id. at 1.
13. See id.
14. Id.
15. See id. at 2.
16 See id. at 4.
18 Id. at 19.
23 See Indictment, supra n. 22 at 2, ¶ 1e.
25 Id.
26 Id.
27 Id.
28 See Press Release, supra n. 21.
29 See Settlement Agreement, supra n. 20 at 1, ¶ E.
30 See Indictment, supra n. 22 at 7-8, ¶¶ 17-18.
32 See id. at 3.
33 Id. at 8.
35 See Settlement Agreement between the United States of America and the Regents of the University of California at 1, ¶ C (Nov. 23, 2021).
38 See Commins, supra n. 37.
39 See Settlement Agreement, supra n. 35 at 1, ¶ D and 2, ¶ 1.
40 Id. at 3, ¶ 3.f.
41 See UCSD Press Release, supra n. 36.
44 See PPOA Press release, supra n. 42.
45 Id.
46 See Settlement Agreement, supra n. 43 at 5, ¶ E.e.
47 See PPOA Press release, supra n. 42.
48 See Settlement Agreement, supra n. 43 at 6, ¶¶ 1 and F.
50 See PPOA Press release, supra n. 42.
51 Id.
53 Id. at 7.
54 See id. at 5.
55 Id.
56 Id.
57 Id.
58 Id. at 6.
THANK YOU to Policy & Medicine Compliance Update.

We currently are accepting submissions for future issues. To submit an article or for questions about the submission process, please contact our Editor, Dr. Seth B. Whitelaw at editorial@policymed.com or visit our website at www.complianceupdate.policymed.com

All materials in Policy & Medicine Compliance Update are for general information purposes and are not intended to be and should not be taken as legal advice. A person’s inclusion on the Editorial Board for Policy & Medicine Compliance Update does not necessarily indicate their endorsement of articles herein. Similarly, quotes included and opinions expressed by attorneys in the articles do not necessarily reflect the views of their firms or their clients or their employers, and should not be taken as legal advice. No attorney-client relationship is created through the purchase of Policy & Medicine Compliance Update or the use of policymed.com. If you have particular questions about a legal or compliance issue, you should seek professional legal advice.