

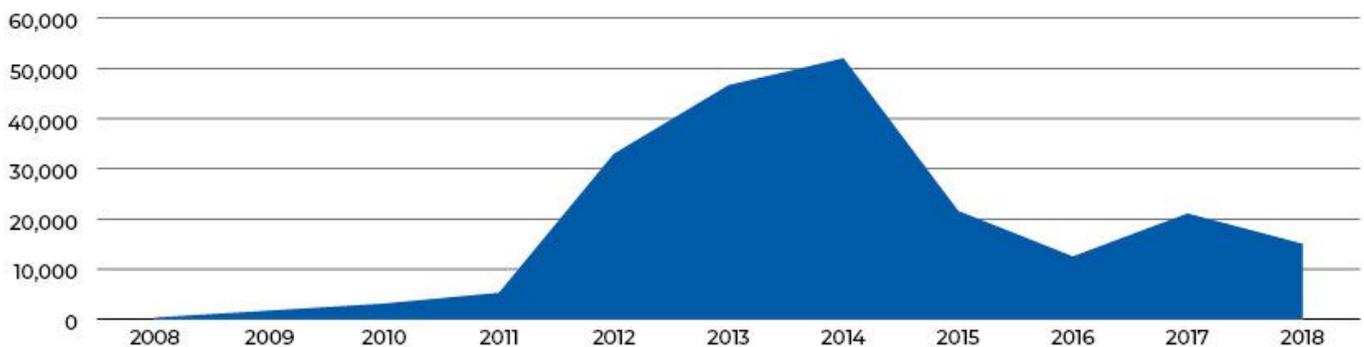
Building Resilience to Anticipated Risks

Tanya Raj

The Global Landscape

Financial institutions globally have paid USD321bn in fines to regulators since the financial crisis of 2007-08, according to a 2017 BCG report. Most of these fines have been in relation to [risks](#) such as mis-selling to clients, internal behavioral misconduct, regulatory breaches, failure to prevent misconduct, inadequate security and safeguards, market manipulation, and failure to maintain books and records.

Global fines and penalties in the past 10 years (USD mn)



Source: Violation Tracker

FINRA's, the SEC's, and the FCA's 2019 themes for regulatory examination also revolve around some of these risks and ways to mitigate them. Foremost among them are firms' culture and governance, financial crimes, technological change and resilience, conflict of interest, cybersecurity, safeguarding client interests, supervision and governance, and suitability.

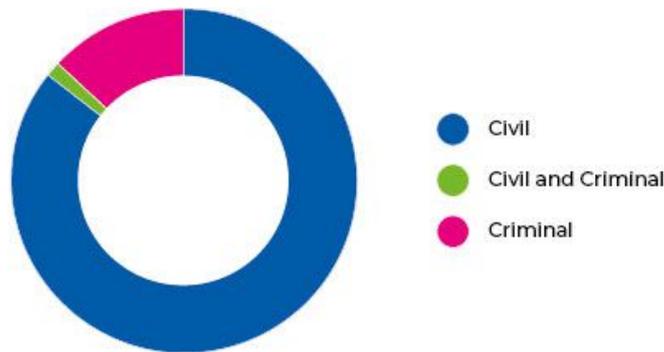
Why Forensic Testing and Investigation?

The data above is a stark representation of how much firms have at stake, not only financially but also in terms of reputational damage, when it comes to risks facing the new world challenges. Companies comprise of individuals, and most of the fines and sanctions can almost always be traced back to bad actors within the firms.

Policies and procedures in place can only do so much in terms of safeguarding a firm's risk, but the ability to test their applicability lies at the core of a robust compliance program. Internal threats could arise from valid human errors, negligence and even white-collar crimes. In the court of law, there is a fine line between being able to prove a firm's innocence and its involvement in terms of

enabling such crimes. Even when proven innocent, firms have sometimes had to make public apologies, damaging their reputation, and shell out settlements that increase each year.

Civil vs. Criminal Fines



Source: Violation Tracker

Today, every firm has its own set of surveillance mechanisms and automated checks that alert it of any misdoing. However, it should be noted that all these alerts are based on a specific set of rules that are fed into the system, with a set of logic functions, and all results are based on past events.

For a firm to be a step ahead of bad actors, it is imperative that it be able to predict risk trends, identify recurring patterns, and anticipate unaccounted-for risks. These areas are currently out of the scope of automated surveillance systems and require human intervention in terms of critical thinking and intuition. This is where forensic testing and investigation come in and provide a much needed service in terms of bridging the gap in identifying such scenarios.

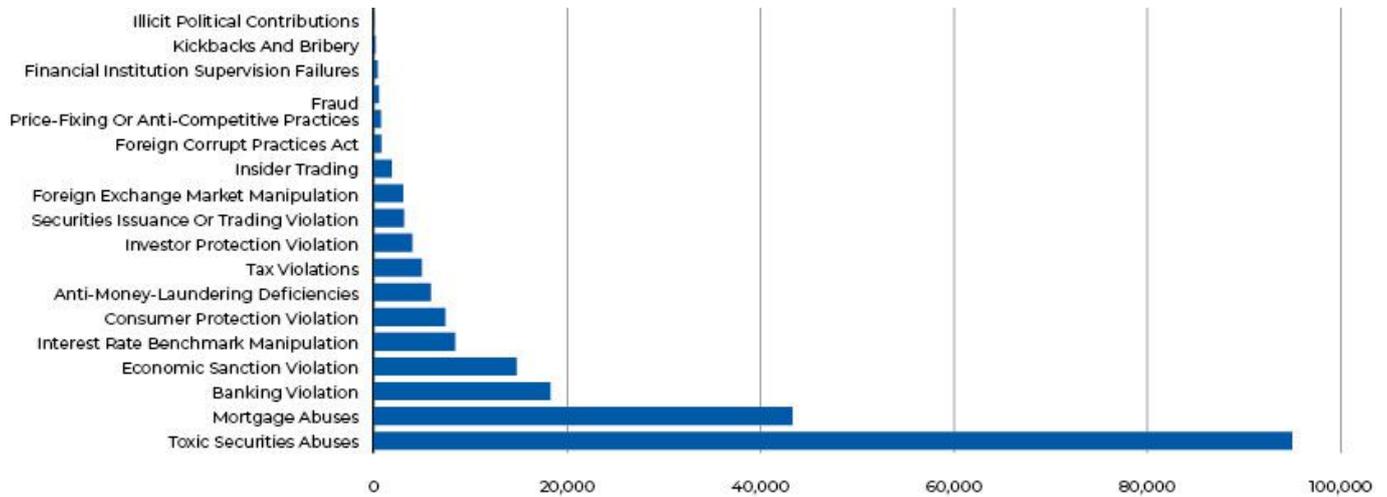
Until recently, the functions of core compliance were a check-the-box activity that firms undertook as a customary task. After the global financial meltdown and recession, compliance as a function has emerged as a key component of lines of defenses and is here to stay. Gone are the days when it was seen only as a point of approval; now, it is a challenge function of an organization, and [forensic testing serves](#) as the independent audit arm of compliance to keep the cogs well oiled.

Readiness and Resilience

In recent years, regulators worldwide have focused increasingly on white-collar crimes. This scrutiny has led to regular checks, translating into mandatory stress tests, regulatory examinations, and supervisory colleges. Participation in the free market and the global financial community now largely depends on how well an organization is able to navigate not only its home-country regulations but also global regulatory standards of operation.

A theme emerging among regulators in 2019 is their collective approach to enforcement actions. From Australia to Europe, there have been calls to take stronger enforcement action on banks for even the smallest of misdoings. The Monetary Authority of Singapore (MAS) published an enforcement monograph in 2018, the Securities and Futures Commission (SFC) has its own specialist enforcement teams, the European Central Bank (ECB) exercises stringent enforcement through the Single Supervisory Mechanism, and the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), along with the Bank of England (BoE), now have Enforcement Decision Making Committees.

Top areas fined, 2008-18



Source: Violation Tracker

Complex issues involving complex human emotions require a human touch. What drives an individual to commit a white-collar crime? What is the motive behind market manipulation? Why do people choose to circumvent the system despite being aware of the policies? Being able to answer these burning questions is the key to mitigating risks before they occur.

Being in the environment, noticing things, reading the mood, understanding the urgency from regulators, acting immediately – all of this builds upon the readiness and resilience of an organization. Forensic testing and investigation, even though at early stages in the financial sector, has been making steady progress in helping firms strengthen their compliance programs and build their defenses.

Looking to the Future

So, where does all this lead? Much has been said about the concept of human touch, but we live in a technologically advanced world, where we are faced with a new invention every day, which could be either a boon or bane, depending on how it is used. We see definite growth in the field of forensics with the help of technology, but rather than a look back, as in surveillance, the sight is forward, as in forecasting risk trends.



Data is the key component, and we should watch for inroads being made in the areas of machine learning and artificial intelligence. Regulators have been deploying these technologies slowly but steadily, and with many players in the market, success would depend on who can provide a solid framework within which machines could learn.

Data remains key – for conducting analysis or for feeding findings into the machines to predict future crimes. Being able to sort, massage, classify, and link data so that it gives the desired results again requires an array of specialists, not only from a technology perspective but also from a domain-knowledge perspective, so that you and your firm reap value for your efforts.

[Acuity Knowledge Partners Solution](#)

Ability to tap into the right talent with the right skillsets is also vital. Forensics is all about people – human reactions and judgement. Forensic testing analysts should be able not only to partner with your team, but also to provide valuable insights from a domain-knowledge perspective. At Acuity Knowledge Partners, we bring you the knowledge, skillsets, and a trove of ideas to kick-start your forensic testing program and keep the wheels turning.

With our focused set of offerings in the areas of [Forensic Analysis](#), Compliance Testing, Monitoring Programs, Risk Trend Analysis, and Risk Mitigation, we customize and design reviews dedicated to your firm’s risks, keeping the latest regulatory expectations in mind. A well-thought-through approach – from initial analysis to end documentation and recommendation – will provide you with a holistic view of your business’s risks and build its resilience to any threat.

About Acuity Knowledge Partners

Acuity Knowledge Partners is a leading provider of high-value research, analytics and business intelligence to the financial services sector. The company supports over 350+ financial institutions and consulting companies through a team of over 3,000+ subject matter experts who work as an extension of the clients’ teams based out of various global delivery centres.

We empower our clients to drive revenues higher. We innovate using our proprietary technology and automation solutions. We enable our clients to transform their operating model and cost base.