The Société Générale/Jérôme Kerviel trial: issues of e-discovery and forensics plus governance, risk and compliance [UPDATED]

June 22, 2010 | By Gregory P. Bufithis, Esq.

Lire cet article dans le français cliquez ici.

Reported by: *Darius Champion, special correspondent to Project Counsel and Gregory P. Bufithis, founder and chairman of Project Counsel*

23 June 2010 — We have had the good fortune these last two weeks to be following the Société Générale/Jérôme Kerviel trial in Paris at the Chambre Criminelle de la Cour which is the criminal court hearing the case. We have been following the case since last September (*click here* for our first post).

Daniel Bouton, former chairman and chief executive of Société Générale (SocGen), who eventually resigned after criticism of his handling of the trading scandal, testified yesterday. He was the last witness to appear before the "summing up". Bouton lashed out at Kerviel in court and repeated his mantra of Kerviel being an "evil genius." He insisted that none of Kerviel's supervisors were aware of his trades. He acknowledged there had been failures in SocGen's risk control system but said Kerviel's ingenuity would have cracked any mechanism.

The trial will end this Friday. Kerviel risks five years in jail and paying 375,000 euros in fines if found guilty.

A note on procedure: *SocGen filed a criminal complaint the day it announced the loss, initiating the probe. The bank will participate in the trial as a civil party, a status that enables it to seek damages under French law. In France, criminal claims precede civil claims, so if Kerviel is cleared, the bank won't be able to seek restitution. It's important for the bank to prevail because it would prove that Kerviel was basically acting as a rogue trader, that this was not an institutional or systemic failure. If he gets exonerated, then it really would call into question management and internal controls at SocGen.*

It has been fun to cover and quite complex but we have had our friend Alain Renoir (no relation to either the painter or the cinematographer) who is a former derivatives trader and he has worked us through some of the arcane concepts. Kerviel has waged a carefully orchestrated media campaign to win public sympathy — rising from relatively humble origins in the French countryside of Brittany to enter one of Paris's most powerful trading rooms to be "just a pawn in a rotten financial system".

The case, the story

In 2008 SocGen announced that it had uncovered €5 billion in losses that officials attributed to the actions of a 31-year-old "rogue trader." The trader, named Jérôme Kerviel, had "managed to evade multiple layers of computer controls and audits for as long as a year, stacking up 4.9 billion euros in losses for the bank." SocGen called Kerviel's actions "pure fraud." The loss is believed to be the biggest in history by a trader. SocGen executives said that Kerviel had an "intimate and perverse" knowledge of the bank's auditing capabilities and back-office operations that enabled him to cover up his unauthorized trades. A French banking governor commented that Kerviel was a "computer genius" and had been able to breach "five levels of controls" at the bank.

But how was he able to evade any detection by other employees or SocGen's trading and auditing systems? If there were controls in place, how is it possible he could have done it alone, as the bank claims? And why did it take the bank so long to discover the fraud?

Following the revelation, Kerviel became an international celebrity overnight, similar to British trader Nick Leeson whose losses brought down blue-blooded merchant bank Barings in 1995. Kerviel's photo swirled around the Internet, and Facebook fanpages were devoted to him. He came out with a book entitled *L'engrenage, Mémoires d'un trader* ("Trapped: Memories of a Trader") which has been a best seller in France. In the most widely circulated quote from the

book he compares financial trading to prostitution: "At the heart of this great banking orgy, traders are only given the same consideration as any street prostitute: a quick thank-you for a good day's takings."

And the case is full of ironies. When the Kerviel scandal erupted in January 2008, the subprime crisis and all its consequences had hardly begun. Indeed, the disclosure of the €5bn trading loss overshadowed at the time SocGen's concurrent announcement that it was taking a €2bn write-own from the US mortgage crisis. Even more ironic was the fact that the trading scandal enabled SocGen to recapitalize itself quickly with a big emergency rights issue before the crisis made this sort of operation much more difficult. And SocGen had just been given an award that January by *Risk* magazine that praised its ability to manage its financial risks.

The gist of the Kerviel case: the "Delta One" defense and SocGen being "in the know"

Kerviel has never denied that he was the sole architect of over 1,000 fake trades, but he insists that his superiors turned a blind eye. The defense is trying hard to prove that Kerviel's direct management at SocGen were in-the-know about many of his unhedged positions. The internal investigators said that Kerviel's bosses also overlooked unusually high levels of cash flow, accounting anomalies, high brokerage expenses, Kerviel's failure to take a vacation and a huge jump in his earnings in 2007, when he reported gains of 25 million euros stemming from proprietary trading. The report said that only 3.1 million of his earnings could be explained by legitimate operations. The trader is also said to have made 500,000 euros on an unspecified one-way bet. The trade breached the Delta One desk's market risk limit (we'll get to Delta One in a minute) and his bosses did not tally the amount into his year-end bonus.

And the fact that Kerviel worked for SocGen's "Delta One" team. Delta One teams are common in most large financial institutions, and they effectively focus on "delta one" products. As the name implies, those relate to derivatives that have a delta of one – products whose derivatives are dependent on equal moves in underlying securities. These can include exchange-traded funds, equity swaps, futures, forwards and so on.

In recent years, these desks have increasingly become merged with banks' general equity proprietary desks. In short, as the *Financial Times* recently pointed out "Kerviel's position was not that of a exclusive proprietary trader, but rather a market-maker who had the ability, if necessary, to make directional proprietary trades — sometimes using the bank's aggregate position for the benefit of his own book". For an in-depth analysis of what these Delta One Teams do and how it impacts what happened at SocGen see the full *Financial Times* analysis by *clicking here*.

Further, as Kerviel testified, he sent weekly treasury reports to his SocGen bosses, bolstering his claims the bank knew about the scale of his trades. In fact, he testified that his supervisors were aware of, and encouraged, his activities. The treasury reports "to me represented a reflection of my activities," Kerviel told the judge. "Every week I made a report and sent it to [my supervisors]." The treasury worked like a small bank for the traders, Kerviel said. He borrowed billions to supplement the 20 million euros he was allotted, based on his trading desk's 125 million- euro limit and paid back interest on the loans, he said. "It was like an internal loan," he

said. In the summer of 2007, Kerviel said he borrowed 1 billion to help while he was in a losing position, then, by July, he was ahead again. "None of my superiors asked questions," he said. They "could see exactly what was in the treasury of each trader."

And according to the testimony of Eric Cordelle, Kerviel's immediate supervisor at SocGen, the Delta One trading desk exceeded trading limits "quite frequently."

But what was interesting from a risk/compliance issue was the testimony last week from Taoufik Zizi, a junior trader who sat next to Kerviel on the Delta One desk. He said Kerviel asked to enter trades on Zizi's computer several times, as well as on other traders' machines, using their log-in information, Zizi said. Kerviel was "a star trader. It's not everyone who makes a million euros a day." (We address the risk/compliance issues below).

Further, Benôit Thaillieu (who left SocGen in 2006 and was supervisor of the Delta One trading desk before Kerviel joined the unit and was intimate with their internal systems) testified that a series of alerts, accounting and trading procedures would have made Kerviel's supervisors aware of the risks he was taking. "For me, it's a certainty," he said. Kerviel's trading profits were extraordinarily high and would have indicated that he was dealing outside his official remit and would have been detected. But the telling point:Thaillieu had seen a multiplication in risk-taking on the trading floor in his seven years at –SocGen — "Profits went up – and so did the risks."

Earlier in the trial Valérie Rolland (a former SocGen compliance officer) had testified that several databases would have been available to Kerviel's superiors where all trading operations could be tracked and that his superiors would also have been able to track down changes made in the data entry system to mask positions.

The e-discovery issues

E-discovery is a relatively new concept in France and most of Europe. But as **Mary Mack** of Fios Inc. has told us numerous times "globalization is resulting in the long tentacles of the American courts reaching across the world. As a result, both foreign companies and the courts are paying attention to electronic discovery". And like several other technology sectors that touch on governance, e-discovery has risen sharply in importance and is quickly becoming a standard defense against the machinations of legal agencies, regulators and other information-hungry forces.

SocGen used software developed by **Autonomy** (the UK-based search specialist) to work out what had been going on with Kerviel and his trades, as well as his communications — the same technology used for early case assessment, document review software, and social media analysis. In fact Autonomy recently launched a product that monitors what is being said on internet social networks, such as Facebook and Twitter. As social media come to affect more businesses, they need to spot potentially compromising blog posts, tweets or online comments. Social Media Governance also helps organizations comply with their own internal policies and new industry-specific regulations governing social media. More on all of this coming up in a longer post tomorrow.

Side note: *in the wake of scandals such as Kerviel's alleged rogue trading or the aggressive rumor-mill that undermined banks including HBOS and Bear Stearns, banks are now eyeing an emerging new range of "spy software" that can even monitor instant messaging dialogue, utilizing powerful computers that can read emails, listen to telephone conversations and analyze chat conversations as participants type. The software that enables the recording and monitoring of employee activity can help companies collect huge amounts of internal information – which they may increasingly need in the face of lawsuits spawned by the subprime crisis, or to meet rising regulatory demands. And in one display of counter-intuitive creativity, French IT consulting and software company LCA hired Kerviel in late April (after he gained provisional release from prison pending trial) to presumably help develop systems to net rogue traders.*

Much has been made in the press and by commentators about the impact of the EU Data Protection Directive (Data Directive) that establishes the regulatory framework for personal data. Laws adopted in accordance with the Data Directive vary, so each EU country has its own privacy twists. EU law treats privacy as a fundamental right, whereas, in the United States, there are no real strict privacy laws. And we certainly know the issues Google is having in France as regards the sensitive data it acquired such as passwords when putting together its Street View service (for more *click here*). That examination was carried out by French data protection agency Commission nationale de l'informatique et des libertés (CNIL) which will decide whether to prosecute the search firm for gathering the data.

In fact in the SocGen case, as was widely reported, bank executives and investigators were loath to look at the Kerviel's email. Even though he was about to bring down the whole company, they were still afraid of the French privacy laws. But based on the investigators' report and the trial evidence, that got over that pretty quickly.

In the Kerviel/Société Générale scandal, employee and executive email and instant message records were critical to discovering what happened. As relayed in court, a forged e-mail purporting to come from Deutsche Bank tipped SoGen that something was up with the transactions being executed by Kerviel. As the bank came to realize he had exposed it to 50 billion euros of potential liability, it rushed to study all of his electronic messages in its possession.

As has been reported in *Le Monde* and the *New York Times* Kerviel rarely used his office e-mail account, sending no more than 60 messages over the relevant time period. But he actively used instant messaging. Drawing on all the available records, the bank swiftly acted to neutralize Kerviel's outstanding trading positions. The bank examined thousands of messages stored from the bank's internal instant message system, including some between Kerviel and a suspected accomplice.

So it showed that SocGen had been storing message records.

Side note: *There are other e-discovery and litigation issues. Assuming the U.S. class action cases go forward after Kerviel's trial and the e-discovery reviews are done within France, there is a good question about the effect of the French blocking statute (blocking statutes are enacted,*

in part, by countries with a purpose of thwarting U.S. discovery obligations). And what of the role of the public relations campaign in France as part of a growing trend to increase the pool of potential plaintiffs in U.S. securities class actions against multinational companies which was examined by our colleague Paul Karlsgodtat his Class Action Blawg (click here).

And just a few additional words on litigation discovery rights and individual privacy rights

During the trial coverage we came across a brilliant book by Matthew Sorell entitled **Forensics in Telecommunications, Information and Multimedia** which includes discussion and analysis of the legal and technical Implications of collecting wireless data as an evidence source. The book also addresses the conflict of litigation discovery rights and individual privacy rights. The SocGen class action cases and other private litigations cross international borders. The conflict of litigation discovery rights and individual privacy rights in different international jurisdictions can present a very challenging situation for litigants. There is a conflict inherent between litigation discovery rights versus individual privacy rights and how different nations deal with this conflict.

At the heart of this challenge are the different priorities that different nations place upon an individual's right to litigate disputes and an individual's right to privacy. Those countries that place a higher priority on the rights of individuals to seek full satisfaction of their claims against other parties than they do upon the right of privacy tend to have much more liberal discovery rights in the litigation process than do countries that place a higher priority on the rights of individuals to retain their privacy. Those countries that value privacy rights over litigation discovery rights tend to restrict and severely limit the ability of parties to litigation to seek information that may be essential to prosecuting their claims in court.

Vey simply put, in the US electronic discovery cases and rules may be changing, may be still undergoing interpretation but one thing is consistent in U.S. discovery rules: if something exists, it is discoverable if the information to be obtained might lead to something relevant. This approach to litigation discovery places the highest priority on having disputes fully litigated in the light of all possible facts that might have a bearing on the issues in controversy.

Litigation discovery rights outside the United States are generally limited by the laws and customs of countries that value privacy rights over litigation discovery rights. In Europe, countries belonging to the European Union developed the European Union Privacy Directive, which is valid in 25 countries. As part of these directives personal data (data which identifies or concerns a specific named person) cannot be transmitted outside the European economic area (EU nations, plus Iceland, Norway and Lichtenstein) to a country which does not provide by national law protection commensurate with the EU.

The EU data directive provides that all computer processed personal data must allow the individual the absolute right to access data concerning themselves, must prove that individuals have freely given consent, the use of the data must be lawful and fair, adequate, relevant and accurate and may be used only as long as necessary and have adequate security. In addition, some countries such as France have criminal statutes known as the French Blocking Statute if information is provided that has not met these requirements.

The main reason for this difference in litigation discovery practices is the difference in various countries' views of personal privacy. Privacy has never been a guarantee in the US Constitution, so privacy rights have developed in a sporadic and unsystematic manner. There is no one comprehensive privacy law in the US, but rather, privacy law in the United States can be characterized as a myriad of cases, statutes, administrative rules that rule on component of privacy. U.S. privacy laws are general and decentralized. To determine the privacy law in the United States one must examine the Federal Trade Commission rules, a variety of federal regulations, various individual state consumer and fraud acts and some sector specific acts such as the FERPA, Gramm Leach Bliley Act, the HIPAA and others.

As Sorell notes in his book "in the U.S. electronic data was everywhere before anyone thought of the implications of this free flowing information. No one foresaw hackers, identity thieves, phishers or pharmers. Once the problems surfaced there were too many well established institutions with vested interests and strong lobbyists who prevented any possibility of stopping the information from continuing to flow. Lobbyists [made] direct contact with members of Congress to influence their views".

And a further reason for different rules is countries' views on the collection of information. In the US discovery is handled entirely by the litigants and outside of the courts involvement unless a conflict occurs. In fact, under the Federal Rules, a litigant "must, without awaiting a discovery request, provide to the other parties… a description by category and location — of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses." In most civil law nations gathering information is a judicial function. The civil law system of courts is based on inquisition rather than the common law adversarial system. The judge normally questions the witnesses and makes a summary of the information. The US system of discovery is unlike most other common law countries.

Now, back to the Kerviel case.

The governance, risk and compliance issues in the Kerviel case

Kerviel's knowledge of back-office computer functions enabled him to conceal some of his bets by offsetting deals with fictional counterparties. He himself said "I had taken too much of a risk, my trading positions were too big. I had succumbed to the intoxication of the numbers game and to the excitement of my job and there were no safeguards to rein me in" in his book.

As related at the trial, Fimat was at the centre of inquiries (Fimat is part of the SocGen Group, a subsidiary of Société Générale Securities Services. Fimat Group consists of more than 1,900 staff in 26 market places and is a member of 44 derivatives exchanges and 19 stock exchanges worldwide). Eurex (the derivatives exchange; for more *click here*) alerted SocGen to suspicious trades by Kerviel. Kerviel used the Fimat name in his cover-up of allegedly fictitious trades. Eurex detected that a supposed Fimat trade was, in fact, initiated by Kerviel from SocGen's Delta One proprietary trading desk. SocGen would later claim that Fimat, although owned by the bank, is an independent brokerage and used that to buttress its central argument that Kerviel had used extremely sophisticated techniques to escape its internal controls.

But was there an apparent break down in financial and internal IT controls subverted by an employee with IT know-how and authorized systems access? Or is this more of a case of eyes wide shut? As Alain Renoir told us, financial institutions of all types are notorious for weakening risk-management procedures when times are good and profits are flowing fast. When he was trading at his bank there was always an executive "game" at play: balancing the potential gains from a risky endeavor versus the potential losses. Taking advantage of opportunities vis-à-vis risk management.

Side note: *one of the best conferences on the whole governance, risk and compliance (GRC) area is the IQPC Corporate Compliance Exchange. The IQPC group is simply at the very top of the game. We just covered their most recent conference and you can see our coverage by clicking here. It is the perfect setting for senior legal and compliance and information professionals.*

And in an area of complexity such as derivatives (SocGen's primary business line, by the way; SocGen had for long invested heavily in residential mortgage-related collateralized debt obligations as well as becoming a leader in derivatives). When it was working, this strategy helped SocGen make a lot of money boosting its market capitalization) whereby a financial instrument allows a trader to make contracts on a wide range of assets (such as equities, bonds or commodities) and attempts to reduce (or hedge) the financial risk for one party in the deal. … well, this necessitates some aggressiveness and can be fraught with risk.

But if SocGen wasn't really as aware of the actual level of exposure as they should have been, why? What the risk managers, and CIOs and IT folks always talk about: the limited interaction between business risk managers and IT risk managers. The old story of "the-business-risk-managers-feel-IT-is-speaking-a-different-language". And "IT-feels- business-managers-don't-really-understand-the-amount-of-IT-related-exposure." This was highlighted by the recent Recommind-sponsored survey of IT managers (*click here*).

In the SocGen case Kerviel allegedly manipulated the IT controls on the business systems based on his mid-office experience and back-office (IT) knowledge and expertise. According to a *New York Times* story the internal SocGen investigation on the incident found at least 75 red flags raised by accountants, and risk-control and compliance officers over a two-year span. These alerts included "transactions that appeared to settle on a Saturday or trades where the counterparty was either not named or listed as 'pending'—from June 2006 to January 2008. These transactions should have alerted managers to Mr. Kerviel's activities" (for full NYT story *click here*).

There is a terrific detailed graphical representation of Kerviel's exploits and SocGen's missteps put together by risk-management vendor SailPoint Technologies that shows just how and where controls should have stopped Kerviel's activities. (The document is entitled "Avoiding a Billion-Dollar Blind Spot" and can be found by *clicking here*).

For example, Kerviel was able to subvert systems access and privilege controls, allowing him to misappropriate names and passwords of his colleagues and mask his fraud, according to the SailPoint document. Quoting the folks who created the graphic: "If at the top of an organization

there really is not adequate division between those who use and manage IT controls and those who are responsible for their supervision and ensuring they're not exploited, then controls may be ineffective."

Consequently, the SailPoint document states that due to its "weak access controls and activity monitoring, [SocGen] was left to rely upon external events to reveal the ongoing fraud rather than their own controls."

So just what can/should IT/Risk/Compliance Do?

If there is anything good that can come out of Kerviel's alleged deviance and SocGen's (apparent? faked?) blindness to it is that the incident will spur executives to talk about risk management and IT controls inside their businesses. Scott Crawford (Research Director and Security & Risk Management Practice Manager at Salient; for more on Salient *click here*) is a bit of an expert on this case and he suggests a "conversation" that can start off with something as simple as asking a series of what-if questions. These include:

• Would you be able to recognize anomalies that would indicate you may have more risk exposure than you realize? Are there events taking place and are detectable in IT that would indicate you might be subject to an event of this nature? If so, what kind of anomalies would you be looking for?

• Are entitlements and privileges for high-level and high-risk employees too broad? Do individual roles or individual users have entitlements that would basically negate adequate separation of duties? Is there adequate insight into that kind of activity? And how effective are the controls assuring that the separation of duties could be enforced?

• What are the behavior anomalies that would suggest you may be facing greater exposure? What is the risk that your control systems or indicators themselves may be subject to subversion? And what are ways you can enforce more effective controls and still be able to capitalize on new business opportunities?

Crawford says one of the biggest issues is the sharing of access privileges by high-level employees. "The issue of the highly skilled professional who is familiar with system architecture and particularly how to infiltrate it is one the biggest risks highlighted in the Societe Generale case."

And it's not just the financial services industry that has had info-security and risk management problems (although with trillions of dollars in play every day, it's bound to bring out the best and brightest crooks). It today's interconnected world, it doesn't matter if the culprit is on the inside or outside, or if a company has the minimum or maximum level of controls—people are too devious and too clever and too resourceful, and they will always find ways to outsmart their computing counterparts. In a brilliant book by Bruce Schneier (**Secrets and Lies: Digital Security in a Networked World**) he talks about the fallacies of digital security mechanisms such as encryption. He reasons that while the mathematical principles and algorithms behind 128-bit key and public-key infrastructure schemes are indeed perfect, the tools "don't exist in a

vacuum." They exist in the real world. And the weak points in security have "nothing to do with mathematics," he writes. "They are in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics are made irrelevant through bad programming, a lousy operating system or someone's bad password choice."

And the trial continues

As we indicated, Daniel Bouton was the last to testify. The trial ends this Friday. The final three days are reserved for closing arguments by the prosecution, civil plaintiffs and Kerviel's defence. We'll have a post-trial wrap-up next week.

Gregory P. Bufithis is the founder and chairman of Project Counsel SCS (http://www.projectcounsel.com). He is also the founder and chairman of The Electronic Discovery Reading Room (http://www.ediscoveryreadingroom.com) and Babel-Law (www.babel-law.com).