Solving Modern Crime in Financial Markets

Analytics and Case Studies

Marius-Christian Frunza

SOLVING MODERN CRIME IN FINANCIAL MARKETS

Analytics and Case Studies

FIRST EDITION

Edited by

MARIUS-CHRISTIAN FRUNZA

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Academic Press is an imprint of Elsevier

Academic Press is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products,instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-804494-0

SOLVING MODERN CRIME IN FINANCIAL MARKETS

Preface

The recent charges by U.S. authorities against Navinder Singh Sarao[1] for market price manipulation contributing to the *Flash Crash* episode in 2010 opened a new chapter in the ontology of crime on financial markets. Sarao's character diametrically conflicts with Jordan Belfort's iconic picture not only in terms of image, but also in term of means, tools, trading style, and technology.

Sarao's "anti-golden boy" case changed in many ways the paradigm of financial markets crime. If a sole trader buying and selling American shares from his parents' basement through a complex network of offshore entities[2] was able to trigger or amplify the 2010 *Flash Crash*, there now have a new type of financial crime that needs to be investigated and a new spectrum of potential threats mainly related to use of technology and cyber-security in relation to the market infrastructures. Whatever the outcome of Sarao's case it is clear that the huge influx of technology in the investment world has brought as many threats as it has opportunities. Hence, financial crime research will need to expand in the coming years to address this and other new types of threats.

In my previous book, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets*, I presented the origins and various forms of crime used in financial markets. The next step is to develop the statistical and data-mining investigation methods that can be leveraged and expanded to analyze crime in financial markets. Forward-looking analysis of financial crimes that can gain momentum in the foreseeable future is also necessary in this context.

This book covers the new types of fraud on financial markets with a focus on cryptocurrency and the sport-betting market. Case studies are presented including the LIBOR and Forex manipulation cases. A set of statistical techniques and exploratory methods is introduced in relationship to various examples of crime. The book aims to present a balanced perspective of theoretical quantitative analysis and applied cases studies and to describe them in a language accessible to the average reader in the areas of financial crime and statistics. The investigation of a financial crime or of a potential threat needs to be accompanied by a good understanding of criminal phenomena along with elements involved in offenses. The use of quantitative analytics alone cannot solely solve a given case and should be paired with strategic knowledge of the crime.

[1] Flash crash trader Navinder Singh Sarao "sat on £27m fortune while his mother worked two jobs" http://www.telegraph.co.uk/news/uknews/crime/11557755/Flash-crash-trader-Navinder-Singh-Sarao-sat-on-27m-fortune-while-his-mother-worked-two-jobs.html.

[2] "Flash Crash" Trader Navinder Sarao Worked With Fund Network Now Under Investigation, http://www.wsj.com/articles/flash-crash-trader-navinder-sarao-worked-with-fund-network-now-under-investigation-1434527646.

Prologue

Despite the recent trends in technology and risk management, quantitative techniques cannot under any circumstances be solely seen as *deux ex machina* solutions for preventing and dealing with financial crime. Of course, statistics, data-mining, and computational techniques can bring more focus or accuracy in valuing the frequency and severity of a financial offense, but a crucial role of analytical methods is to provide tools for determining the causes and cradle of crime rather than predict its outcome.

The consequences of crime on financial markets in the past two decades have extended beyond the investment world and started to have a considerable impact on the real economy. The manipulation of agricultural commodities prices or interest or Forex rates can have a serious impact on the economy and even contribute to political turmoil and social unrest in certain countries or regions of the globe. The massive role played by technology in markets infrastructures adds new threats to the investment world mainly related to cyber-security issues and ultra-low latency trades.

In this context of increasing opportunity for crime, regulators, investigators, and institutions exposed to financial markets need to have appropriate methods and systems in place to detect or to find abnormalities in markets. The philosophy of such a framework should be forward-looking since the *leitmotif* of financial crime changes quickly and a static threat assessment framework would not be able to address new types of offenses. Therefore, existing statistical and data exploration methods need to be employed in a dynamic framework with learning abilities in order to tackle crime on financial markets. As past cases have shown, the various crime typologies are generally interconnected. For example, low latency market manipulation might be linked to money laundering and therefore the analytic methods need to be integrated in a holistic way.

The main challenges of addressing the variety of threats in financial crime are related to both theory and implementation. The theoretical challenges concern the choice of appropriate methods for tackling an offense and the implementation-related challenges concern the right way to build processes and systems for surveillance and detection within an organization or a market infrastructure.

Acknowledgments

The author would like to gratefully and sincerely thank Didier Marteau, Chevalier de l'Ordre National du Merit (Knight of the National Order of Merit), Michel Mouren, Derek Cunningham, Leslie Pitts, Evgueny Kurinin, Piotr Ryzenkov, and Erika Bigg for their support.

The author is also grateful for the academic contribution, input, and support of:

- the Laboratory of Excellence for Financial Regulation in Paris (LABEX-ReFi) represented by Prof. Didier Marteau, Dr. Christian de Boissieu, and Francois Gilles Letheule for providing access to the databases (IODS, Barclays Hedge, Bankscope, Financial Times, and Bloomberg).
- Dr. Evgueny Shurmanov from the Ural State University for his continuous support and scientific collaboration.
- Dr. Aurora Castro Teixeira from the University of Porto for her efforts of organizing the most cutting-edge conference in financial crime to the Interdisciplinary Insights on Fraud and Corruption (I2FC).
- Dr. David LEE Kuo Chuen from the Singapore Management University for the cutting-edge insight on cryptocurrency.

The authors also thank Laura Hutton for her precious insight of financial crime. The author is grateful to Scott Bentley for making this project happen and to Susan Ikeda for her continuous support.

David Lee Kuo Chuen: Interview

London, United Kingdom, April 5, 2014

BIOGRAPHY

David Lee Kuo Chuen—Ferrell Asset Management Pte Ltd., Singapore Management University, Singapore

David Lee Kuo Chuen is Professor of Quantitative Finance (Practice); Director, Sim Kee Boon Institute for Financial Economics; and Academic Director, Global Master of Finance Dual Degree at Singapore Management University. A Chartered Statistician from the Royal Statistical Association, he received his Ph.D. from The London School of Economics and Political Science, University of London. In May 1999, David Lee founded Ferrell Asset Management Pte Ltd. Prior to setting up Ferrell, Dr. Lee was the Managing Director of Fraser Asset Management, the fund management unit of the Fraser-AMMB group of companies. He also served as Director of Institutional Sales at Fraser Securities and covered the Asia-Pacific equities markets.

Marius Cristian Frunza (MCF): *Why is Bitcoin different from classic currencies and from other electronic currency?*

David Lee (DL): It is different because cryptocurrency is not just a currency. There is a lot technology in it. A lot of people think that it is money, and that is true, but it not just money. It is programmer's money, and therefore has great potential flexibility. You can do what the program asks you to do. With Bitcoin 2.0 or Blockchain 2.0, for example, one might implement functions that are currently out of reach. Take a look at the many opportunities in smart-accounting. One simple example is that an artist can allow everybody to own his or her song. If you use cryptocurrency as a kind of token everybody can be a cryptoequity holder of the song. If somebody plays it, you will have a crypto dividend paid in cryptocurrency. This is the beauty of a programmable currency.

MCF: *Can cryptocurrencies be a new investment asset class?*

DL: At this moment cryptocurrencies are very volatile. One cause of their volatility is that the transaction levels are low, even though $8 billion in Bitcoin is changing hands. In addition, 60-70% of Bitcoins have not transacted in the last 6 months, according to the latest report. If prices are too volatile they cannot be treated as an alternative asset. You can look to the direct exposure to technology through venture capital and in start-ups through private equity way, but investing in Bitcoin is not a new investment alternative class on its own. When prices stabilize, Bitcoin will make more sense because of its predictability. Now it's difficult to value. Bitcoin is still an experiment that can go to zero, but it has a lot of upside. We see a lot of evolution in technology and new cryptocurrencies are emerging that are capable of tasks currently out of our reach.

MCF: *What is the role of hardware in transacting cryptocurrencies?*

DL: There is one thing about cryptocurrency that makes it special. Originally cryptocurrency was intended to be distributed in the network; in other words, every node would have equal access. Cryptocurrency was to be a democratic experiment in the sense that each node participates to the mining and at the same time

participates in updating the transaction digital registers. But as the experiment has progressed developers have realized is that some people have better machines and higher hash rates, and they are better prepared to solve the cryptocurrency contest. They can form pools as mining costs rise, giving them further advantages. Some people can be left out in the confirmation of the public ledger. Like every democratic system, some people will tend to have more means and be able to influence other who are followers.

MCF: *Can cryptocurrency be sustainable without central banks?*

DL: I think it will coexist with central banks. Two contrasting cases are possible. At one end of the spectrum are governments that have a lot of debts. Their currencies are not reserve currencies, and there is a danger that if they run into problems people will lose confidence in their currencies. At the other end of the spectrum you have countries with lots of reserves. These countries are forming a different monetary system, as China is with BRICS banks and bilateral swaps. The Asia infrastructure bank is trying to set up a new financial system. What happens is that some governments have so much debt that they will need set up their own cryptocurrency at the country level. Their cryptocurrency will be geographically limited whether it is backed by tangible assets or other currencies. I see there is a road for those cryptocurrencies and cryptocurrencies like Bitcoin to co-exist together. If governments regulate, they can regulate the intermediaries but they cannot regulate the cryptocurrencies protocols. A lot of regulators try to understand the technology, but it evolves from day to day. The regulatory crime busters are always behind in this race. Cryptocurrencies will continue to exist with their own values for transactions complementing central government currencies.

MCF: *Would it be possible for a government to adopt a cryptocurrency as an official currency or in parallel?*

DL: I think what will happen is that governments will begin regulating intermediaries and alternative investors such as hedge funds. Those who are currently part of the system will then become the mainstream, libertarians who do not want to deal with regulation will exist in another space. Therefore, the cryptocurrencies will have two main groups mainstream and libertarian non-mainstream. The mainstream will develop much faster due to the governmental support. But the protocols will still exist as they are, and I think this experiment will end positively. Conditions will continue to evolve, and cryptocurrencies will both adapt to changes in the environment and will drive a lot of innovation. The best brains and the best developers are in that space, so you can expect innovation on an almost daily basis. That is interesting. Any government that encourages innovation will not turn down a cryptocurrency that creates something that benefits mankind. If you do not look carefully, cryptocurrencies will disrupt a lot of industries, such as banks, payment system, spot exchange, and ownership in the form of shares. Cryptocurrencies will be part of a new digital economy. For this reason I don't think governments will ban this cryptocurrencies. It is not a wise thing to do.

MCF: *What is the risk of cryptocurrency transactions being related to protocol?*

DL: One of major dangers is that cryptocurrencies involve mining, and whoever controls more than 30% of mining will have some influence. Whoever controls more than 51% can actually have a major say in rewriting the latest block chain. This could make the digital registry untrustworthy. When there is no trust in the cryptocurrency protocol the price will drop and people will abandon it. Few will be mining, and no reliable record will exist. That is the danger of minable cryptocurrencies. But there is another consensus, ledger cryptocurrencies, which are decentralized and don't need mining. For example, you could have 30-40 parties

forming different nodes and agreeing on a digital ledger. I think those areas will see a lot of development. Non-minable cryptocurrencies are an area to look into as they do not pose the same danger that exists in minable cryptocurrencies.

MCF: *What is the risk of theft and hacking in the cryptocurrency world?*

DL: You can always have protocols such as proof of state or proof-of-identity and limit the mining revenue, reducing the consumption of more electricity. Regulation wise it is unclear that if somebody steals something from your computer you have the right as a property owner to go after him. Data and cryptocurrencies are digital assets. It will be interesting to see how regulations or propriety rights will be revised to address this point. The other consideration is that a cryptocurrencies are generally unregulated. They are easy to attack, like stealing coins from the intermediaries. In this context consumer protection is a key issue. Watch for new attention focused on property rights for digital assets and consumer protection in the next one or two years.

MCF: *The consumption of electricity for the mining process is high and the electricity price is a key factor for mining profitability. Will we see a concentration of miners in low electricity price countries?*

DL: These activities are already happening. Most of the farms are located in Asia, where electricity costs are lower. That's how we had a few miners controlling close to 51% of Bitcoin mining earlier this year. This concentration in itself is a danger. If mining costs go higher individuals will give up mining on their own and will join a pool, which again poses a threat of consolidating 51% of mining in the hands of a few. We can see mining moving to farms that have low electricity charges. Rental costs are also important because you cannot mine in big cities with high rent prices.

MCF: *Media has noted the risk of money laundering. What are your views?*

DL: Money laundering through cash or other financial instruments is always with us. At the same time, technology development around cryptocurrencies will continue to be innovative. People in the business of financial crime will always have to catch up with innovation. Cryptocurrencies are probably not the best way to launder the big money because transactions can be easily tracked. Cryptocurrencies are not a avenue for laundering big money; people can move only small amounts, and it is possible that people can actually move money in bigger portions. If cryptocurrency intermediaries are being regulated, if the main stream of cryptocurrencies is being regulated, and if the Bitcoin community is working to together, it will be much easier to target those illicit activities.

MCF: *What are the main competitors for Bitcoin?*

DL: One of them is XRP by Ripple, which is used by financial institutions for transactions. In XRP's case there is a ledger book of consensus, so you don't need to have all the processes Bitcoin has. You will see a lot more such innovations coming out and you will see also new kinds of cryptocurrencies such as country-based or regional cryptocurrencies with their own particular interests. Major cryptocurrencies will co-exist.

MCF: *Will we witness a new generation of cryptocurrencies less intensive in terms of protocol?*

DL: I see proof-of-identity where identity is associated with digital imprint, encrypted in that sense. This function is particularly useful if somebody wants to obtain the identity of the person using the currency. Other desirable opportunities include signing contracts by using cryptocurrencies and cryptoequity. They do not necessary involve mining but they do require proof-of-identity, not necessary based on a token, but rather based on a ledger. They would be a variation of Bitcoin that would evolve over time and we are already seeing its first phases.

Laura Hutton: Interview

London, United Kingdom, April 5, 2014

BIOGRAPHY

Laura Hutton—Director of Banking Solutions, Fraud & Financial Crime Advanced Analytics Business Unit (AABU), SAS

Laura is a director in the banking solutions team at SAS, working across the EMEA and AP region, and is responsible for the design, build, and go-to-market processes for SAS's fraud and financial crimes solutions.

Working with companies globally, Laura provides subject matter expertise across the full client engagement process from both technical and business perspectives, ensuring that SAS solutions always drive value for their customers. Laura has a specialist interest in the areas of Rogue Trading, Application Fraud, Trade Finance Fraud, Insider Fraud, FATCA, AML, and Online Fraud.

Prior to joining SAS in 2012, Laura spent 6 years at Detica NetReveal where she was responsible for the development of NetReveal's social network analysis solutions, specializing in techniques to identify and prevent fraud within the insurance and banking industries. When she left Detica she was Head of the Global Banking & Markets practice.

Laura has a First Class degree in Mathematics from the University of Durham.

Marius-Cristian Frunza (MCF): *For over three decades SAS has been a leading provider of analytic solutions for financial institutions. What are the new challenges for the industry in the era of big data, high-speed Internet, and ultra-high-frequency trading?*

Laura Hutton (LH): Let us look at unauthorized trading (the case of SocGen or the case of UBS) in which people hide their positions and their Profit and Loss. How have organizations protected themselves over the last 10-15 years? They have developed control frameworks that identify weaknesses, then they have established controls to tackle those weaknesses. One example I often cite is canceled or amended trades. Canceled and amended trades are frequently associated with high-risk trading events. So control programs identify all cancelations and amendments on a daily basis. We routinely ask our Front Office supervisor to sign off those cancelations and amendments, to say that they are fine. Now the reality is that if you are a Front Office supervisor you may well get 300 to 500 cancelations and amendments on your desk each day. You are asked to review an Excel spreadsheets and say: "Yes. Perhaps one entry corresponds to high-risk trading." You can imagine how difficult that is for a Front Office supervisor. You are looking at hundreds of rows and it is almost impossible to see which rows are fake trades and which are just business as usual.

Cancelations and amendments are just an example. You have another control that queries whether your trader is logging in at strange times during the day or night, whether she has fluctuations in her P&L, whether she has broken credit limit breaches against a counterparty, and the like. In the end there are many siloed areas in an organization, and each is running its own reports. So as a supervisor I not only receive reports containing hundred of records, but I also get 20, 30, 40+ reports on my desk everyday from all the siloed areas of my organization.

Despite everyone's best efforts this Front Office supervisor has a process-driven approach rather than one that enables him to find true exceptions. The human eye is unable to join together these disparate pieces of information. So the siloed nature of the business is very challenging. Many controls are simplistic in their calculations because they are siloed. If I am a clever trader, I can quickly learn to get around rules because SAS uses an "if" decision branch. Recent cases of unauthorized trading are good examples. Traders know the conformation process and can estimate how long they have to cancel a trade after booking it. They would also know how much credit to put against counterparties on fake trades. Where there is a rule, people find a way around it.

Those are the key technological challenges that we are addressing. The only other challenge I would mention concerns the cultural side of things. I do not mean the psychology of a real trader. Instead, I am referring to communication breakdowns among Front, Middle, and Back Office staff. Front Office traders concentrate on making money. But Back and the Middle Office staff must challenge Front Office traders about reasons for cancelling specific trades. Busy Front Office staff often do not provide complete details when describing their trading strategies, which can be difficult to understand even under the best circumstances. Therefore, the difference between Front Office and Back Office means that Back Office does not have really all the information to ask the right questions. If I were explicitly told that a trader did X, Y, Z over the past three months, that he demonstrates this type of activity, and that he did this over here, as Middle or Back Office staff member I would have more of a foundation on which to build my questions. At the moment the typical staff member asks about individual events in isolation.

MCF: *Since the big scandals involving financial crime allegations, major analytic software companies started developing solutions for detecting and providing information about financial crimes. Is this a point-in-time regulation-driven effect or will it become a core strategic development axis in the foreseeable future?*

LH: There is definitely regulatory pressure. Since the UBS case, a lot of major banks have conducted reviews of their anti-unauthorized trading measures and now rate themselves on a red, amber, and green scale. You will also find that while the Socgen and UBS cases attracted significant media attention, all organizations now have internal warning flags. These flags respond to regulatory pressures because if the banks have events, however small, they must report them to regulators. If market abuse is a regulatory requirement like Anti-Money Laundering, unauthorized trading is not. Banks need not file a report for regulators unless they have an event. When banks have an event, they come under considerable pressure to do something.

So the regulatory side is one piece, but there is also the reputational side. I think the reputational side drives things more than anything because it includes the fear factor. After Leeson nobody thought it will happen again, then Kerviel happened and nobody thought it could happen again, and then the UBS Adoboli case happened. It was a copy of the SocGen event. At that point a lot of people looked carefully and said that the same thing could happen to them. The financial loss did not concern them as much as the potential damage to their reputations. Since the financial crisis most big organizations have increasingly emphasized the protection of their reputations. Smaller organizations are perhaps still on that money-making curve or might be more willing to take on risk. We do not work as much with hedge funds because while they have very similar needs they also have a bigger appetite for risk than large international banks.

MCF: *What aspects of financial crime are currently addressed by the industry and what are developments do you foresee? Is there a specific focus on financial markets (e.g., securities, commodities) and market surveillance?*

LH: Fraud and financial crime are huge topics. If you look at retail banks, many use technology and analytics to combat them; investment banks have less interest in these tools. Retail banks have real-time transactions systems to protect against credit and debit card fraud. We have seen a large increase in application fraud, which differs from credit risk in that somebody takes money from the organization with the intention of never repaying it. Traditionally banks have analyzed credit risk and have been very good at credit risk analytics and scoring. But they are not as good at application fraud. We have also seen an increase in internal fraud, which often includes stealing for a customer, targeting elderly clients who do not have good access to their bank accounts, or colluding with vendors. Instances of collusion, or procurement fraud, is the focus of a lot of our work in South Africa and India.

Online fraud is an interesting topic. Take the United Kingdom, where you have expectations for faster payments through an increase of Internet banking. Everybody with a smartphone conducts online banking transactions, and smart phones are clearly a weak point for protecting against fraud. Banks naturally want to deliver good experiences to all of their customers. The challenge is how to give to your good customers good experiences without leaving yourself vulnerable to attacks by bad customers. We see this conundrum in all situations, from Internet banking and online transactions to online lending applications. If you apply online, you immediately become anonymous to that organization. As a good customer this system pleases me because I can apply for my loan from anywhere, but it also enables bad customers to protect themselves behind their computers. Corporate lending, which is a big part of the retail banking business, requires a more manual application process. The techniques are simple and rules based, and often a lot of data are in unstructured formats. We use our analytic capabilities to join structured and unstructured data so we can predict which loans are likely to be targets of fraud.

MCF: *With the "Big Data" wave institutions are creating data warehouses for various types of information, from portfolio metrics to client data and from OTC positions to social media feeds. What are the challenges for the exploration and exploitation of information held in these repositories?*

LH: This is a topic that puts everything into context. These organizations are very siloed in terms of data, systems, and the groups that run those systems. Everything is separate. I have seen organizations create grand 10 year plans to build big data warehouses, and these plans are illogical because it will take them a lot of time and money to bring those data together. In fact, these organizations might need to analyze those data now instead of in 10 years, and they might already be able to analyze the data where they sit *in situ*. What these organizations need is a system that deals with volume. So, for example, in an investigation of unauthorized trading one common strategy is to join up the dots across that organization and thereby analyze a trader's actions. So you have let's say 80 different systems sitting separately: everything from Teradata Oracle and Excel spreadsheets to csv files. The ideal system should be able to sit across all of those formats and ingest from where it sits. Once it has ingested those data, it should be able to draw conclusions. For an internal threat I want to the system to able to say this is the trader and this is everything she has across my siloed systems. The equivalent in an external threat is saying "this is my customer and this is everything I understand about my customer." This is what we describe as creating the holistic picture of your customer or your employee.

We can go a step further by adding information about the relationships my customer or employee has. We want to know, for example, that our employee talks to this trader by phone, she emails that researcher, and she trades on that book against that counterparty. So we create X in the context of all the relationships she has. We do exactly the same thing when we look to external threats. Of our customer Y, we can point

to her loan application, her accounts, all of her transactions, and related information such as her address, the names of people she lives with, her telephone number, the names of people who receive money from her, the ATM machines she uses, and so forth. We create the social network, and I am not talking about Facebook or Twitter here. I am talking about a true social network, a fraud network analysis. Once you have that view you can apply your risk assessment.

Let's return to the unauthorized trading example. I have trader X and I know the book she trades on, the counterparties she deals with, the trades she has made, and all the controls she has ever broken. I know the relationships between her and other traders or other people within the organization. Across this view we can apply a range of techniques to detect high-risk activities.

It starts with the most simple rule. A rule could be trader X canceled more than N trades in the last days, or it could be that we joined silos and to observe toxic combinations. X has canceled a trade that was unconfirmed by a counterparty or X has had an increased number of cancelations plus she has not taken her annual leave, plus she started suddenly logging in late after everybody else has gone home. That type of analysis looks for predetermined scenarios. SAS have a catalog of scenarios and our banks have the same. We can use everybody's knowledge, but this tactic uncovers only the events you set out to discover.

Then we use data mining and data analysis to look for events of unknown patterns. If I have a holistic image of X I can analyze her. I can understand via strategies like segmentation or clustering who X should look like, and I can identify her peer group. And therefore I can recognize her deviations from the norms of her peer group.

MCF: *Are classic econometric tools and analytic frameworks appropriate for the analysis and detection of financial crimes? Is there a place for a new forensic science/discipline dedicated to the behavioral and analytic study of financial crimes in order to develop a specific theoretical background?*

LH: The techniques we use are exactly the same as those we follow in other contexts: ingesting the data, linking them together, and applying risk assessment.

We use this process for tax and VAT carousel, insurance and claim fraud, first-party bank application, unauthorized trading, and market abuse. We use SAS's traditional analytical techniques, employing segmentation clustering, which have been around for a number of years. What is different is combining them to generate data, then analyzing the data. That is what we describe as the detection piece, and it is new in that space.

The other piece we address is access to the underlying data and speed of access. So traditionally data has been seen as an enemy of organizations that want to tackle fraud. My view is that data should be a friend because if you can to use data in the right way, most of the warnings signs you need are in the data. You have to be able to harness the data in the right way.

The fundamental principle of SAS approaches is to harness the data. On one hand it is an automated detection piece: generating the data and linking them to scoring and alerting. On the other hand it is giving people a window into those data in order to explore and analyze them in better ways. In traditional reporting tools there is a high dependency on IT. Data are stored in a nice format in a nice data warehouse, and they required IT to configure a report for you. We have taken another approach based on in-memory technology that allows you to access a million if not a billion records in seconds. As a business user you can drag and drop pieces of information instantly, giving you the power to answer questions about our business. When I started to work in this area I was often looking for swings in the P&L, shifting from very positive to very negative, steadily going up, or slowly dropping. What we didn't consider was exactly the opposite. More unusual is when the P&L is completely smooth. Should I expect my P&L to be smooth when those in my peer group are not?

MCF: *SAS solutions are widely reputed for their ability to deal in a robust and efficient way with statistical data analysis. The financial world and especially financial markets introduce a "real-time" dimension where speed is a factor. What are the challenges of the solutions meant to detect and prevent financial crime in light of the increasing speed of transactions and operations?*

LH: With all of my clients I think carefully about data analysis techniques. My first question is "do I need real time?" So if I do need real time, what do I mean by real time? What do I need real time for? I need it for credit and debit card transactions because I want to stop the money; if someone's card is in the machine, I want to terminate the transaction or the payment on the internet. So it is a real-time problem in terms of the subsecond problem. Take something like application fraud. An application for a loan will never be given a note in a sub-second. Some banks from Eastern Europe want to be aggressive in order to gain market share. They want to process applications in 30 seconds or maybe in 1 to 10 minutes, which is a near real-time problem, so it doesn't need the instant response of an online transaction but it does require quick action. Other problems do not develop as quickly, such as an unauthorized trade, internal fraud, or procurement fraud.

These last problems do not manifest as quickly so you do not need to spend money to accelerate the response. In these cases what you have is a batch problem near real time. In real time, such as credit and debit card transactions and high-frequency trading, where one-thousandth of a second makes a difference, you have grades. The faster you need to respond, the most expensive and bigger the hardware you require. So you need to work out what speed you actually need and you need to use the appropriate hardware. With fraud and financial crime we offer platforms that allow everything from batch to real time and near time. Organizations can address all types of financial crimes on one platform, and they can chose their analytical and reaction speeds. The faster they want to analyze and react, the more complex hardware they need.

MCF: *In the current environment "money laundering" has become a multinational/multi-asset phenomenon. Can analytic solutions bring answers alone or is expert input required? What is the right balance and the right way to mix them?*

LH: I do not see a challenge of mixing them as long as they are used in the right ways. As a business user I explore some data and might well identify new behaviors that are not in the automated systems. What I learn should be fed back into my automated intelligent system. Actually, I would like to look for this toxic combination scenario or look at a new analytic method that automatically defines it. I think they sit very nicely side by side as long as the right operating model is in place.

Mathematical or quantitative people need to run these analytics. A business expert who understands fraud and financial crime needs to guide those scientists to ensure you are not just running blind analytics, but you run with domain expertise in mind.

MCF: *For the behavioral understanding of financial crime mechanisms, Bayesian techniques and machine learning offer many upsides. How robustly can these methods be implemented in specific solutions?*

LH: All fundamental tools and techniques are applicable to financial crime, but that is not to say that technology should become stationary. Visual analytics is a new way at looking at data.

In terms of techniques, I think there is an increasing importance in dealing with unstructured data. SAS has traditionally used numeric data, but we also use a lot of nonnumeric data, linked text, and unstructured text to capture risk. Let's take the example of unauthorized trading for which the unstructured data analysis is very important. A lot of the banks look at the analysis in isolation, like a separate project. I don't agree with this approach, as it is part of the larger story of identifying the bank's trader and what he is doing that poses a risk to the organization. We

use text analytics to join structured and unstructured data, extract them, and link the relevant information. And we go through understanding the sentiment of unstructured information to derive the risk that trader is posing. In unauthorized trading we see a strong correlation between people who cancel or amend trades at unusual hours with those who have an increase in the sentiment of urgency or mismatching between Front Office and Back Office emails. We have to be able to make the data available. In terms of analytics we use a lot of developed analytics techniques to analyze the risk. What is new is the way we link the data together. That creates the holistic image of the trader and is fundamentally new in concept. We have a greater volume of data and evolving insights in ways to link data together.

I would add that while techniques such as neural networks, decision trees, and logistic regression or segmentation have existed for some years, we are using those techniques on a new platform that delivers high performance analysis.

SAS high-performance analytics have grown in recent years to the point where we can use vast volumes of data. Those data are needed because banks want to deliver better customer experiences they do things more quickly. As we get into the big data arena, where we go across million and millions of records, unless you have a scalable high-performance analytic platform you will not be able to deliver that experience. Some open source analytical platforms do not have the scalability and they cannot take in all the information at once. We have addressed that by taking our expertise in analytics and moving on to a high-performance environment.

There are few other points I want to address. You have to be very careful that your techniques are not black box. What I mean is that if a system pumps out a result saying this transaction is high risk and has a score of 1000, how does this help an investigator? It does not. We need to use techniques that present a case and actually guide investigators in why something is high risk. So the results need to be concise and informative. As an example, for unauthorized trading space we generate an alert that says trader X is high risk because she broke rules A, B, C, plus she is not allowed in that space, plus analytically her behavior has changed over the past three days. Through the risk assessment process we use a combination of rules bases and deep analytical-based techniques and we're still trying to integrate that in a way that business people can understand. Investigators of these alerts are not mathematicians so they cannot be given blind analytics.

It is also important that investigators should be able to manage this information on a continual basis. Let's take the example of anti-money laundering, where it is important to have full audit ability from back to front. You need to know why things are high risk while others are not. Therefore, the whole process must be an open or white box rather than a black box. You need to know the scenarios that are and thresholds that are in place. You need to be able to configure and change those variables. Every organization in every country requires different types of information and their requirements are constantly changing, particularly for crimes like AML. Only an open system enables you to change and adapt over time. Certain techniques are more appropriate in certain situations. In some parts of the business some tools work better than others. For credit cards, neural networks are effective in identifying high-risk transactions. If application fraud, neural networks work less well. You are much better using decision trees or logistic regression with predetermined scenarios for those instances.

In unauthorized trading, you don't have the advantage of known outcomes to set against the predicting model, but you have a vast quantity of data that define norms. Seeing deviation from those norms is easy. So the lesson is to understand your business problem first, then choose the best techniques to detect that fraud. Because

ultimately all we want to do is find the most fraud before the money is lost. For example, first party fraud was typically discovered after the fact, after the money was gone. Why look in the collections book after the money is lost? When you use logistic regression or decision tree analysis to predict what application or what insurance claims are most likely to be fraudulent, you stop the money before it disappears.

MCF: *For financial crime detection many solutions are specific to each intuition. Financial crime is a transnational, cross industry phenomena with global challenge. Can we imagine an industry consortium that shares the efforts for combating financial crime via big-data mining and analysis?*

LH: This is interesting thinking. In fraud and financial crime we have data privacy laws that often prohibit the sharing of information; every country seeks to protect the rights of the person. In fraud and financial crime investigations there are more lenient terms about what you can share. We work with a number of insurance consortia who share their claims and policy data across organizations for the sole purpose of detecting serious organized crime. There are a number of countries globally that are doing it and many more looking into it.

Banks are generally not willing to share their infrastructure because it often means sharing their data. If banks would share data across organizations, we would be able to determine who is defrauding those organizations because we would not only have the full list within a bank but also the full list across a country or countries. I do not think we are there yet, perhaps due to sensitiveness of data and competitive advantage.

In general we have seen a variety of anti-money laundering systems, fraud systems, and sanctions systems in countries worldwide. These systems do not talk to each other. We are working with a number of global organizations to consolidate the outputs of those fraud and financial crime systems. For instance, there are AML systems that generate alerts and fraud systems that generate alerts. In Mexico you have one system and a different one in the United States doing the same things. We are taking gray data, as we describe them, and linking them together at a global level, then determining what countries are missing information by looking at things in isolation. We describe this approach as a safety net proposition. It is not ripping and replacing the existing current systems. But assuming I am in global banking and I have a lot of local subsidiaries, I want to take the output of financial crime and fraud systems and link them together to make sure that they are doing everything possible to protect the business. We call it a global financial intelligence unit.

MCF: *Classical solutions for fighting financial crime have been focused mainly on credit card fraud, transaction fraud, securities fraud, and the like. Where do new markets (Bitcoin) or new industries (the betting and online gambling industry) fit in?*

LH: Banks have a lot of credit and debit cards. Banks are seeking enterprise-wide strategies and they looking at a range of business problems, including trade finance, fraud application, and online fraud. They want to optimize their anti-money laundering systems and create financial intelligence units. But this drive is not limited to banks. We do a lot of work with insurance companies on claims fraud, policy fraud, and changes by product. At banks we typically look at unsecured loans, unsecured lending, credit cards, overdraft, and personal loans; and we concentrate on portfolio-secured lending such as mortgages and on commercial business loans such as trade finance fraud. In claims, investigators used to look at motor and home insurance, but now people look at life insurance, worker compensation, and general liability. We do a lot of work with governments around VAT and carousel frauds, tax fraud. Governments want to diversify into pension fraud and benefits fraud.

I was recently with a large Asian casino that was starting to address issues such as anti-money laundering and fraud in casinos. Even if we aren't talking to Bitcoin, I went to a lecture recently on Bitcoin where people