SPECIAL REPORT: FINDING THE TRUTH

The role of a forensic accountant continues to evolve. With more data to crunch and fraudsters to catch, forensic accountants are now using smarter tools to assist them in tricky cases. Experts in this specialism tell Jeremy Chan how they approach investigations, and why they are now required to master these technologies – or risk falling behind

Illustrations by Gianfranco Bonadies

Imagine having to dig out a single financial statement – with an alleged illegal transaction – hidden among thousands of folders in a cramped back office, all on a tight schedule. This was often how fraud investigations took place when Keith Williamson started out as a forensic accountant 20 years ago. "It was like finding a needle in a haystack – a ridiculously painstaking process," says Williamson, Managing Director at Alvarez & Marsal, a member of the Hong Kong Institute of CPAs and also the Forensics Interest Group Management Committee. "By human error alone, you still might miss that document you were looking for."

The job nature of a forensic accountant has evolved. With more companies opting to store information – especially financial data – in hard drives, servers and the cloud, forensic accountants rely on specific forms of software to solve cases today. Indeed, with 95 percent of business records globally now created and stored electronically, the forensic seizure and analysis of electronic data has become a fundamental process in virtually all corporate enquiries and dispute resolutions, according to PwC. Typically, the role of a forensic accountant involves assisting courts, lawyers and clients to understand complex financial and accounting issues, and presenting that information, to solve legal cases. Investigations aim to resolve financial disputes, which can range from securities fraud, insurance claims, personal injury claims, shareholder disputes, employee thefts, to divorce cases.

Irene Siu, Associate Partner, Forensic and Integrity Services at EY, a member of the Institute's Forensics Interest Group Management Committee and an Institute member, notes that more companies today are taking measures to prevent cyberattacks, and rely on forensic accountants to provide solutions. "We do a mix of proactive and reactive work nowadays," she says. "We help our clients to identify situations based on experience working with other companies and having seen different fraud schemes of possible breaches and loopholes."

The demand for forensic specialists remains strong, particularly with fraudsters using new methods in a bid to outsmart investigators and buy themselves time, says Felix Kan, Senior Manager, Cybersecurity and Privacy at PwC and an Institute member. "Hackers are smarter now – instead of just simply accessing a file, they also make it hard for us to recover data from a hard drive," he says. "For example, they know exactly which files to delete during the hack in order to delay an internal investigation process in catching them."

This special report explores various aspects of one of the accounting profession's specialist areas – forensic accounting. It looks at the latest developments in the tools and techniques that forensic accountants use to detect and prevent fraud; how they work with other specialists such as lawyers and cybersecurity experts; what companies should do to prepare for the first interaction with forensic specialists; the key skills forensic accountants should have, and how to get into the specialism; and factors that may shape their role in the future.

TOOLS TO DIG DEEPER

Data analytics as a fraud prevention tool is now the norm for forensic accountants. The process involves identifying patterns of fraudulent activities from large sets of raw data in order to draw conclusions which are further investigated. Specialists also use artificial intelligence (AI) programs to process large amounts of data, or automatically construct charts and diagrams to display crucial information, such as dubious transactions or email threads. "If you're a young forensic accountant and you have skills in data analytics, you're a hot commodity," says Williamson, who heads his firm's disputes and investigations team in Hong Kong and China.

During a recent investigation into a United States-listed company, Williamson's team was tasked to go through six years' worth of financial records. They used robotic process automation (RPA) software Galvanize to filter out the most suspicious transactions. The software analysed general ledgers, accounts payable and receivables, employee expenses and payroll.

"It gave a risk score to each transaction made. So rather than looking at millions of them and supporting documentation, it allowed us to focus on the ones posing the highest risks," Williamson says. "This helped us to build a risk profile model and provide our client with a list of the most high-risk customers, suppliers and employees." This approach, he adds, not only proved effective, but saved his clients time and money.

Chris Fordham, Founding Member of the Institute's Forensics Interest Group, a member of its management committee and an Institute member, notes that forensic accountants now use technology-assisted review (TAR) software to quickly sift through files. "The software learns which keywords are relevant, and in which circumstances. It uses a form of analytics on top of 'e-discovery'," Fordham says, referring to electronic discovery, or the act of completely copying data off a computer's hard disk drive for analysis. TAR uses data analytics and machine learning to sort through millions of documents, sometimes terabytes of data to filter out suspicious documents.

Thomas Fu, Director of Risk Assurance at PwC China, also relies on various e-discovery and TAR software such as EnCase, Nuix and Relativity to image, or copy data off a computer's hard disk drive. These tools made it possible for his team to easily copy information from more than 200 computers during a recent investigation. "The e-discovery tools processed a lot

"If you're a young forensic accountant and you have skills in data analytics, you're a hot commodity."

of electronic data, mostly emails and files. We absolutely need these tools, especially when looking at unstructured data," he says, referring to computer-based data such as emails, word processing documents, spreadsheets, videos, photos, audio files, presentations and webpages. "It uses AI and machine learning to determine whether certain keywords in emails are related high-risk keywords which might be linked to fraudulent activity," he says.

Forensic accountants also use software with predictive and prescriptive analytics capabilities which use machine learning to predict outcomes based on data, and advise investigators on courses of action. Annie Chan, Partner and Managing Director of Corporate Recovery and Forensic Services at Mazars Hong Kong and an Institute member, says the firm recently acquired machine learning software company Zettafox, and uses its software's AI capabilities to predict the odds of fraud occurrence. "We instruct AI what to analyse and what results we want," she says. "For example, if a company's expenses are ever-increasing and reaches a stage where it looks suspicious, it will automatically notify forensic accountants."

There are also tools to identify bribery. Katy Wong, Partner and Head of Forensic at KPMG Hong Kong, former member of the Institute's Forensics Interest Group Management Committee and an Institute member, uses a tool to create a chart, similar to a mind map, by scanning emails for evidence of fraudulent activity. "After inputting electronic records into the AI tool, it automatically clusters all the records based on conceptual similarities. It shows the potential individuals suspected of paying bribes and the people they are corresponding with the most. We can quickly see if there are any suspicious communications between the suspect and people outside their organization," says Wong. Investigators can then focus on particular connections directly on the chart and view conversations.

During a recent investigation, Wong used the software to verify the claims of an interviewee. "Our suspect denied having any communications with a particular supplier – but the tool helped us identify related documents," she says. "That allowed us to probe deeper."

Edwin Hui, Director of Data and Analytics, Management Consulting at KPMG, utilizes the visual capabilities of the data analytics tool in anti-money laundering (AML) cases to track how criminals electronically "layer money" – or move funds to separate accounts to avoid detection. "In AML, you have 'layers' of people laundering money for you, so it was previously very difficult visualizing the relationship between certain individuals," Hui says.

"If you trade using cryptocurrency, how do you prove those transactions are yours?"

Forensic accountants and virtual currency

The rising prevalence of virtual currencies such as bitcoin, present new ways for individuals to commit financial crime, and will make it difficult for forensic accountants to trace assets. Virtual currencies offering a degree of anonymity allow criminals to move financial assets across jurisdictions without government oversight or regulation.

A weak password opens up possibilities for hackers. In January, hackers stole over US$54 million worth of virtual coins just by guessing weak wallet passwords. Fraudsters have stolen more than US$227 million from exchanges worldwide so far in 2019, according to *Cryptocurrency Anti-Money Laundering Report, 2019 Q2* from software solution company CipherTrace Inc.

While Hong Kong's Securities and Futures Commission imposed a set of regulations to govern virtual currencies in November 2018, forensic accountants expect to take on more cases involving the recovery of cryptocurrency assets because of increased use. "We're moving towards a cashless society, and cryptocurrencies are going to be among the most used currencies within the next 5-10 years," says Irene Siu, Associate Partner, Forensic and Integrity Services at EY.

Because every single transaction in the cryptocurrency system is recorded in a digital ledger, known as a "blockchain," forensic accountants can currently use traditional methods, such as investigating transactions in the cryptocurrency ledger or work with cybersecurity specialists to analyse Internet traffic through particular servers and Internet Protocol addresses. Though existing methods may work for now, the next generation of forensic technology – and forensic accountants – will need to devise ways to efficiently oversee more cryptocurrency transactions. "Unlike cash, it isn't physical, so this raises many security concerns."

Cryptocurrency ownership is another problem, as multiple individuals could have the password and be able to access a wallet. "Because access and ownership go hand in hand, it's a challenge proving that you are the sole owner of your virtual coins," says Jack Jia, Forensic and Integrity Services Partner at EY. "If you trade using cryptocurrency, how do you prove those transactions are yours? We are already being asked by companies to design software to prove that they own their virtual coins."

The tool detects anomalies, which are shown as outliers on the chart, and shows the different accounts and individuals that criminals are working with to launder money. "We can essentially pinpoint the ringmaster, and even see the transaction details between ringmasters and their subordinates among different major groupings." With more evidence to work with, forensic accountants proceed by interviewing suspects to see whether their claims corroborate with their findings. Chan from Mazars says: "We interview relevant individuals such as management, staff members and even vendors to collect more information. This can lead to further investigations. We are often asked by our client to provide a fact finding investigation report with forensic analysis as well as a conclusion."

Jack Jia, Forensic and Integrity Services Partner at EY, says programs are indeed changing the landscape for forensic accountants by cutting down on repetitive work and pointing investigators in the right direction. He uses AI-based platform EY Virtual to detect stock market manipulation, such as spoof trading, where a trader places a large order to buy or sell a financial asset, such as a stock or bond, but with no intention of executing it in order to move the market price. The trader would then place hundreds or thousands of smaller orders and profit from the cancelled order.

He uses the software's machine learning capabilities to develop models based on its results. The software, works round the clock to detect spoof trading activity and creates a graph, where potential spoof traders appear as spikes. "By looking at past spoof trading patterns, we are able to develop more algorithms behind this platform to identify spoof traders," he says. "You still need an investigator who understands these patterns and is able to explain them to a programmer."

According to Y L Cheung, Forensic Leader at Deloitte and an Institute member, forensic accountants often work with banks on AML cases and now use robotic process automation (RPA) tools to alert them when unusual transactions going through a bank's system is detected.

Employees would usually have to investigate and report suspicious transactions to the Joint Financial Intelligence Unit, a joint unit run by the Hong Kong Police Force and the Hong Kong Customs and Excise Department – though some of those transactions would usually turn out to be false alarms upon further investigation.

"Before we started using RPA, people had to go through endless records. It is now able to eliminate those false alarms," Cheung says. "For example, if a customer performs a one million dollar transaction every month, the software learns this sort of behaviour. But a one-off transaction of a large amount of money will set off alarms, and by looking at records, the robot is able to discern between suspicious and non-suspicious transactions." RPA, however, still needs to be programmed by a human forensic accountant. "Technology is adaptable, but every case is unique. It takes a human being to understand the background of the case and know what to look for before programming the software," adds Fordham. "At the end of the day, we need to be able to discuss the findings with the individuals and decide whether we need to dig deeper or conduct interviews to have suspects explain discrepancies which were found via the software."

WORKING WITH OTHER SPECIALISTS

With increasingly complex forms of fraud, forensic accounting involves a lot of cross-profession work, whether it's with technology professionals or lawyers.

"Generally, complex forensic accounting engagements will feature a law firm because there is usually a legal or disciplinary side," says Guy Norman, Value Creation and Crisis Management Partner at Deloitte China Financial Advisory, Convenor of the Institute's Forensics Interest Group Management Committee, and an Institute member. (Read more about him in the Leadership Profile feature on page 22).

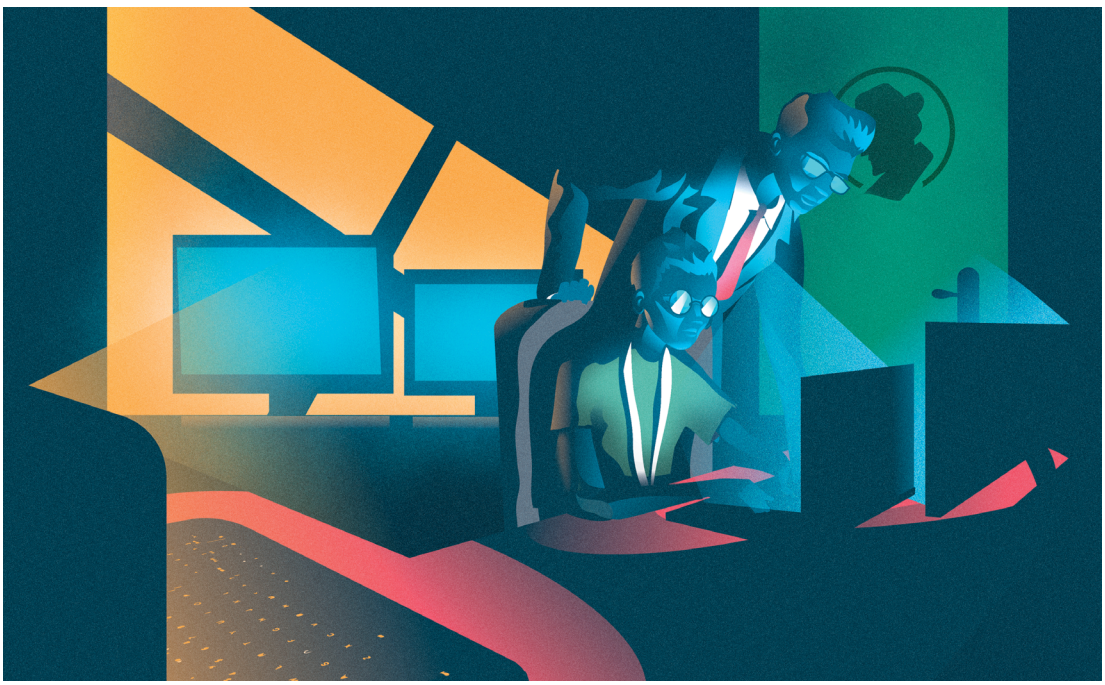
He adds that the line between the professions is blurring. "Because of the broadening of both the legal and accounting professions in the past decade, there is a lot of competitive behaviour between us and many of the areas have merged. A lot of accounting firms, ourselves included, might also have relatively small legal practices and the law firms have equally tried to grow their own expertise in the accounting side of investigations."

This not only increases competition for winning business, but also creates issues over who does what. "A lot of us who are a bit older would like to go back to those old days where everyone knew where they were, and we weren't competing," he says.

Fu and his team at PwC frequently work with cybersecurity specialists to clamp down on cyber fraud, especially within banks and companies. He has seen an increase in schemes involving criminals hacking into the email account of senior employees, posing as a chief executive officer or chief financial officer of a company, and asking employees within the organization to transfer money to a specific bank account. "In these cases, the cybersecurity team determines whether the email servers were indeed hacked by a fraudster, if they had knowledge of the password, and which emails were looked through. They would also identify which emails were sent by the hacker and which were really sent by the CEO," he says. "Often times, several emails are sent through the CEO's account, instructing the finance staff to transfer money to the hacker – who might even be using different bank accounts. Forensic accountants then have to analyse the bank transactions and quantify the losses."

Employees within the organization are most susceptible to deception, and there are cases where there is no actual hack to begin with. "A hacker could even use a different – but similar looking – email address. For example, they might replace a lower case 'L' with the number one, or a lower case 'O' with the number zero," says PwC's Kan.

Many companies in Hong Kong lack adequate cybersecurity measures to prevent such attacks. A staggering half of businesses in the city reported a cyberattack and 23 percent have no measures in place against them, according to the 2018 study *Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World*, which surveyed 1,300 mid-sized and large businesses.



"Because of the broadening of the services offered by the legal and accounting professions in the past decade, there is a lot of competitive behaviour between us."

WHAT COMPANIES SHOULD EXPECT

Companies need to play their part and work closely with forensic accountants throughout a fraud investigation, which can involve frequent meetings, provision of information and contacts relevant to the case, and the correct preservation of digital data for analysis. In addition to forensic accountants, companies can expect to work with a team made up of individuals who specialize in law enforcement, external and internal audit, and computer forensics.

Investigations tend to begin with a meeting between the company's board of directors and the forensic team to discuss the issue at hand. "We need to understand the company's operations and controls to determine the nature of the fraud and where it might be concealed," says Chan of Mazars. Fordham adds: "In every investigation, the forensic accountant needs to get a full understanding of what the issues are, how the issue was discovered and the ramifications of that issue." Many investigations will involve a legal aspect. "We would ask whether the company needs to engage a lawyer, for example, in order to preserve legal privilege," says Siu from EY. Fordham adds: "More often than not, the company has its own internal general counsel's office. If they do, they will oversee and direct the investigation to maintain a sense of control over the output of it." Additionally, companies would be expected to provide accurate details such as their legal and financial structure, methods of production and purchasing, flow of funds through the business, employee compensation methods, accounting and control systems and procedures, and whether accounting records had been properly maintained.

The investigators would produce a plan which lists the possible outcomes and methodologies used in the course of the investigation, and a timeline which must be agreed upon by both the company and the forensic team. "Any investigation plan needs to be flexible and adaptable in case things change – such as new information is discovered," says Fordham.

It is important for companies to appoint a person of contact, usually a member in upper management or legal counsel, who will work closely with the investigators throughout the investigation. "We have to gather information such as policies, procedures, documents and data from computers and servers," says Fordham. "That person has to be the single point of contact, and has to assist in making the necessary arrangements for the investigators to do so, and for us to speak to people who may hold information. It's a critical role." Investigators may request documents such as internal audit reports in relation to the case or an organizational chart, to help them better visualize relationship hierarchies and also perform background research. "We'll also give them a list of people we want to interview," he adds. Siu adds that companies also need to consider how the investigation may impact the day-to-day operations

of the business. "If the investigation is going to be conducted discreetly, the company needs to consider how to deal with the employees who are under investigation."

Forensic accountants would also begin the process of collecting data. "We might spend the first few days or weeks capturing and preserving all relevant document and electronic data for further investigation," Fu at PwC says. "Any forensic accountant will require prompt and complete access to data and documentation at the company to be able to perform their work as completely and efficiently as possible," says Williamson of Alvarez & Marsal. "Companies should expect there will be significant demands on their time and resources from the forensic accountants, particularly at the outset of the investigation."

Companies will have to provide all relevant information to the forensic accountant for further inspection, and both parties need to sign a non-disclosure agreement, adds Fu, who says this is done as soon as possible, in order to prevent data being deleted or tampered with. In order to convict a defendant of a crime, the evidence against them must be handled in a meticulously careful manner. Both parties will also expect to sign a chain of custody during the investigation, which is a chronological document stating the collection, sequence of control, transfer, and analysis of the electronic data. It documents each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. This ensures that the evidence can be used in a court of law. Cheung from Deloitte says: "Depending on the complexity of the fraud scheme, we may need to spend a significant amount of time performing detailed data analytics work on relevant databases such as hard drives and servers."

Investigations can stretch over weeks or months, and it is crucial for both investigators and the company's management to hold regular talks to discuss findings, resolve issues or obstacles and to ensure the agreed scope remains relevant within the investigation. "Such meetings should be much more regular during the early stages of the investigation, when most is learned and can be shared across the team, and decisions will be made that will frame the scope, timeline and cost of the rest of the investigation," says Williamson, who adds that a good forensic team will be looking to build strong and collaborative working relationships with key members of staff.

Forensic accountants also need to deal with third parties and rely on their cooperation of banks, customers, suppliers and individuals beyond the organization's control. "Clients generally want the answer immediately, so forensic accountants tend to work under a lot of pressure," Fordham adds. "It's our job to explain and manage the expectations of management as to why an investigation may take longer than expected – especially when it comes to extracting additional information from third parties." Cheung says: "Companies should try not to exert pressure on the pace of the investigation work, its scope, or how the investigation report should be worded."

At the end of an investigation, forensic accountants might be asked to present their findings in a report which covers the scope and objective of service, investigation approach, key findings, conclusion and recommendations. Long reports can be costly, and investigators may be expected to present their findings and results in a meeting.

"It wouldn't be remarkable for someone to join my team and find themselves in a different country the following day."

A day in the life of a forensic accountant

Day-to-day tasks vary, and work is done on a project basis with cases taking weeks or sometimes months to complete. Most forensic accountants agree that their jobs are diverse, and often times, unpredictable. Katy Wong, Partner and Head of Forensic at KPMG Hong Kong, sometimes starts her mornings by tending to a new case. "I might get a call from a client who has been subject to a cyber attack. I would then need to arrange for our cyber response specialists to speak to their IT department immediately to gather more information about what might have been discovered, and then suggest to the client how we can help them to contact the attack, understand analyse the root cause, and mitigate the damage." After lunch, Wong could be asked to review a report, such as an advisory report on financial crime compliance, before it is submitted to a client. Later that day, she might be meeting with senior partners to discuss budget plans for the following year's technology infrastructure, recruitment needs, and business development strategies.

Because no cases are the same, forensic accountants formulate a unique strategy before undertaking a case. "Unlike an audit, there are no typical steps or work programme for a forensic accountant to follow," says Irene Siu, Associate Partner, Forensic and Integrity Services at EY. "Research is a big part of our job, for example, we perform background checks." During investigations, they gather financial evidence, identify perpetrators, quantify losses, interview suspects and often serve as expert witnesses in courts.

In addition to handling cases locally, forensic accountants often need to travel abroad to meet with clients and interview suspects across multiple locations, sometimes on short notice. "There are days where the client needs your assistance, and it wouldn't be remarkable for someone to join my team and find themselves in a different country the following day. It can be stressful, crazy – but it can be a lot of fun," says Chris Fordham, Founding Member of the Institute's Forensics Interest Group.

THE SPECIALIST SKILLS NEEDED

Forensic accounting not only calls for individuals who are fluent with numbers, but are also inquisitive, analytical, and able to put themselves in the shoes of others. "It's almost like we need people who are able to think like a fraudster – and even one step ahead of them," says Siu at EY. Cheung adds: "We aren't looking for people who follow a checklist. We want people who will do what it takes to find the truth."

Forensic accountants should also have good verbal communication and people skills, and the ability to tactfully interview suspects. "We deal with all sorts of people – regulators, law enforcement, stakeholders, and we need people who are good at gathering information." There are both informational and confrontational interviews in forensic investigations. Informational interviews help to provide more insights into business operations, internal controls as well as the personal roles and responsibilities of employees. Confrontational interviews are more formal, and usually involve potential suspects or individuals who have knowledge the investigation team wants to obtain. "They can be asked to recall particular transaction, communications and events, and are often asked follow-up questions with reference to supporting data and documentation," says Williamson at Alvarez & Marsal.

Chan from Mazars agrees, saying that interviewing and extracting key information from suspects is an art. "At first, you need to establish rapport with the interviewee so they understand what you are doing and find reasons to tell you the truth," she says. "We might spend the first few minutes having a casual conversation or even talk about the weather, depending on the type of interview. We inform the interviewee who we are, the purpose of the interview, and what we need from them. We need to be quick to respond and ask follow-up questions to obtain the crucial facts we require." Fordham says: "You need an enquiring mind, and you can't accept anything at face value – a bit like an auditor."

Also like auditors, forensic accountants must be detail-oriented. They must perform adequate research before interviewing suspects, or risk being taken advantage of. "Interviewees can mention things you might not understand, so you need to prepare beforehand, such as by understanding the company's background, the products they sell, and their operations," says Chan. "You don't want your interviewee to see that you haven't got a clue about what they're talking about."

Williamson stresses the need to maintain composure during intense and nerve-wracking interviews. "Your heart may be racing on the inside, but you have to look like you're still in control. If you've lost your nerve and shown that you've lost your nerve, it will be harder to get them to confess any answers you need." Carelessness is not an option on the job, he adds. "Forensic accountants need to know the consequences and severity of getting things wrong. Based on our findings, people might be dismissed, or have legal action taken against them. You really need to get things right."

With the increase of cyber fraud around the world, forensic accountants with cybersecurity skills and knowledge are increasingly sought after. "Going forward, we expect to see forensic accountants who are specialists in cybersecurity, and cyber specialists who are forensic accountants," says Siu at EY. "We hope for those two roles to be indistinguishable in as early as three to five years."

Cheung at Deloitte says the firm has already started looking for individuals with both skills. "We are in the process of building our cyber-forensic capabilities and are looking for professionals – especially juniors – who are skilled in both."

Despite all the technological advancements, forensic accountants should mainly use technology to their advantage and not fully depend on it, notes Cheung. "These software programs may show certain trends or patterns, but they won't always give you the smoking gun. They are meant to provide direction during an investigation," he says. This means specialists should continuously develop their skills in interpreting and summarizing complex financial and business transactions. "It's a specialist field that machines won't be taking over anytime soon – if anything, clients rely more and more on us forensic accountants to interpret what these machines find," says Jia from EY.

Those looking to specialize in forensic accounting can start by joining the Institute's Forensics Interest Group, which provides a platform for individuals in forensic services as well as newcomers to learn about the latest developments in the field. The interest group holds monthly events such as seminars, discussion forums and networking events. "Attending the group's events and speaking with forensic specialists is going to give you a real head start in the profession," Fordham says. Siu adds: "Anybody with an interest in forensic accounting who wants to know more is welcome to join. It's a platform for practitioners to exchange ideas and to speak with professionals in the industry – you'll learn what it's like to be a forensic accountant and also the current issues we are looking into."

"It's a specialist field that machines won't be taking over anytime soon – if anything, clients rely more and more on us forensic accountants to interpret what these machines find."

THE FUTURE

As long as there is business competition, fraud will always exist in one form or another, says Siu, and so there will always be a need for forensic accountants. In addition to greed, factors such as pressure to meet ambitious targets could lead to fraud. "For example, a member of staff – especially senior-level staff – may face pressure when it comes to meeting target revenues and shareholder expectations. This may create an incentive for them to commit that fraud, for example in order to secure additional investments." Fordham adds: "With so much economic uncertainty and geopolitical risks on the increase, this creates pressure on businesses to achieve results. Sometimes, good businesses go out of business, and bad businesses create results to maintain operations. Fraud will never simply go away."

The specialism faces new challenges such as the increased use of virtual currencies (see *Forensic accountants and virtual currency* on page 14) and dealing with data stored within the cloud. "Because more companies use cloud computing, forensic accountants need more tools to extract evidence from the cloud," says Fu from PwC. Organizations that store data such as business records in the cloud without a backup in a server can bring about major problems, especially when criminals hack into a company's cloud server. "Ideally, the investigators want to retrieve and download all emails and financial data from the cloud to their local computers. But nowadays, criminals may delete the original data from the cloud," he says.

The inevitability of fifth-generation cellular network technology (5G) will also speed up the rate and intensity of cyberattacks. 5G will be up to a hundred times faster than current fourth-generation networks and support more bandwidth, making it easier for hackers to access more data from more devices. "Hackers are already fast. They have the skills to move a large amount of files – even from several computers at once – even before someone realizes they have been hacked," says Kan of PwC. "And with 5G, the bad guys will be even quicker," says Deloitte's Cheung.

Chan from Mazars says the latest advancements have breathed fresh air into the specialism, and she encourages CPAs looking for a change in pace to consider it. "Many new forensic accountants are auditors looking to try something new, and a lot of them find it to be more interesting and exciting than routine accounting work," she says. "Things are moving very fast with new developments in technology, so I really hope we get more young professionals to join."

Ultimately, the evolution of the specialism stems not just from its recent technological advancements and diverse role, but from the passionate individuals in the profession who never tire of exploring new and better ways to help clients and companies stamp out fraud. "It's a very dynamic job," says Wong at KPMG, "even though I've been a forensic accountant for more than 20 years, I still find it fun."

The Forensics Interest Group organizes seminars on topics of interest to both forensic accountants and those looking to join the field. Find out about forthcoming events on the Institute's website.

Also, look out for our upcoming video series featuring interviews with forensic experts on the Institute's social media platforms to learn more about the specialism.