

ACAMS[®]TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

EMERGING FINANCIAL CRIME THREATS FOR 2018



Reprinted with permission from the
December 2017–February 2018 | Vol. 17 No. 1
issue of *ACAMS Today* magazine, a publication of the
Association of Certified Anti-Money Laundering Specialists
© 2018 www.acams.org | www.acamstoday.org

ACAMS[®] | Advancing Financial
Crime Professionals
Worldwide[™]



TOM KEATINGE



PAUL TAYLOR



DAVID FERBRACHE

As the techniques used by criminals continue to develop and become more sophisticated, what are the most significant threats faced by the industry in 2018 and which measures and developments will play the biggest role in addressing these threats?

ACAMS Today spoke with Tom Keatinge, director of the centre for financial crime security studies at the Royal United Services Institute (RUSI), David Ferbrache, technical director at KPMG, and Paul Taylor, head of product marketing for financial crime compliance services at SWIFT, on their views about the financial crime threats affecting the industry and the possible solutions.

ACAMS Today: *While regulation becomes more robust, criminals are also becoming more sophisticated. Overall, are banks in a better or worse position to tackle financial crime than they were a year ago?*

Tom Keatinge: Banks have an increasing awareness of the financial crime threats they face and can thus design responses more effectively than ever before. Furthermore, the integrity of the financial system is being continuously strengthened as the partnership between banks and the public sector develops.

Arrayed against these positive developments is the acknowledgement that criminal elements will always adapt, probing for weaknesses in the system that they can exploit. Nevertheless, the collaborative nature of financial crime fighting today puts us in a much better place to identify and disrupt dirty money and bad actors.

Paul Taylor: The industry increasingly recognizes that a 'tick-box' approach to financial crime compliance isn't enough. Regulators now expect banks not only to understand how their compliance systems work, but to also demonstrate that their

programs are effective. These developments mean that banks are in a stronger position when it comes to fighting financial crime, but that they are also facing additional costs and, potentially, risks.

David Ferbrache: Where cybersecurity is concerned, banks are becoming much better at putting fraud controls and analytics in place across digital mobile platforms. They're collecting more information about who customers are, their patterns of activities and how they interact with the banking applications environment. That gives us a richer fraud control and monitoring environment than we might have had previously.

However, what is worrying is the more sophisticated end of cybercrime, where we see banks and financial institutions actively targeted, payment systems being manipulated and larger cash outs occurring. We're also seeing that as banks become slightly more difficult targets, the attacks are moving to the client base, with large-scale CEO and business email compromise fraud being carried out against banks' customers.

AT: *With smaller scale lone-wolf terrorist attacks becoming increasingly common, to what extent are anti-money laundering/counter-terrorist financing (AML/CTF) processes effective against this type of attack?*

TK: The current response to terrorist financing was designed after the 9/11 attacks in New York and in Washington, D.C. Whilst there has been some fine-tuning in recent years in response to the threat of the Islamic State of Iraq and the Levant (ISIL), the global response to terrorist financing does not reflect the extent to which the threat has changed—nor does it reflect the way finance and financial services have evolved.

Too much time is spent by policymakers urging financial institutions to cut off terrorist financing and not enough time is spent exploiting the high intelligence value inherent in financial transactions and

relationships. This is all the more the case when one considers the challenge of identifying the tiny amounts of funding required to buy knives or rent vehicles to carry out the sorts of attacks we have seen in Europe in recent years.

At RUSI we run a new project called "Rethinking CTF" that is precisely aimed at identifying and addressing the gaps in the current response to CTF. What might have been appropriate following 9/11 is clearly no longer enough.

AT: *How can the sharing of financial intelligence between banks, regulators and law enforcement enable financial crime to be tackled more effectively? What are the possible pitfalls or limitations of taking this approach?*

TK: Banks have information and governments have intelligence with which that information can be illuminated. Relying purely on the banks to spot illicit finance and bad actors is suboptimal. For example, by briefing banks on completed investigations and prosecutions, governments can educate banks and thus harden the financial system against similar future events.

Where questions are rightly raised is where the sharing of information between the public and private sectors moves beyond typologies and open source data to include names and other personal information. However, in systems such as the U.K.'s Joint Money Laundering Intelligence Taskforce (JMLIT), close control is placed on the extent to which such personal details can be shared. Where criminality and security is involved, most people would, I suspect, be supportive of this type of collaboration with appropriate oversight.

DF: While information sharing is relatively well established in the fraud community, the cyber information sharing community is much less mature. It can be less clear what the exchange structures are and what the legal basis is for those information sharing arrangements.

It sometimes feels like we have two different communities—one with fraud control, AML/CTF and know your customer, and

the other with cybersecurity and its own threat intelligence, analytics and detection methods. What's needed is a more integrated approach. For example, sometimes we'll find indicators in cyber communications, which give us hints about what those groups are targeting, thereby linking to fraud controls and countermeasures in the other community. We're only just starting to connect the dots properly.

IT IS ESSENTIAL TO GLOBALLY RAISE THE BAR ON BANKING SECURITY

AT: *To what extent are regulatory changes supporting banks in addressing financial crime?*

PT: New regulations, such as the EU Funds Transfer Regulation 2015 (EU FTR 2015) and the New York Department of Financial Services (DFS) Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, are putting more pressure on banks to demonstrate the effectiveness of their compliance programs. While this inevitably brings additional challenges, complying with the new rules doesn't have to be a sunk cost and can help banks address financial crime more effectively. For example, banks can take advantage of the DFS rules to build more robust compliance regimes.

TK: Intelligent regulation, drafted to strengthen the system and tested to consider unintended consequences (such as de-risking) that encourages greater financial integrity, should be welcomed. An example from the U.K. is the Criminal Finances Act that legislates (amongst other things) for information sharing between banks. This new law was created with close consultation with the private sector. Laws and regulations drafted in isolation without reference to the financial sector will, almost always, result in less effectiveness than is anticipated.

DF: Aside from regulation focusing directly on financial crime, it's worth noting that the Revised Payment Service Directive has the potential to transform the financial services landscape by opening up the range of institutions that can access people's financial data. While this is a major stimulus for the community, it does of course raise a lot of new potential attack routes. A new suite of institutions will be handling rich sets of data and will be able to initiate transactions on behalf of individuals, which means these new players will also be introduced into the fraud control community.

AT: *How are cyberattacks evolving and how can banks best defend themselves against the threats? Is cyber set to be the next focal point of regulation?*

DF: Incidents like last year's attack on the Bank of Bangladesh, as well as recent ATM jackpotting attacks, suggest that organized crime groups are trying to find weak points in the international financial system that they can exploit.

It is essential to globally raise the bar on banking security. If we don't get this right, counterparties will begin to say they are concerned about the nature of a transaction, or the integrity of the institution that is initiating the transaction. As a result, they may decide not to do business across the full range of banking activities or they may decide there's a premium attached to certain types of transactions. That's a concern.

I also think we're going to have to deal with the question about where liability rests on fraudulent transactions. In retail banking, banks usually refund any fraudulent activity on customers' accounts, unless it's obvious they've been negligent in their handling of personal credentials. But for industry customers, the situation is more complex. There's a debate about how much risk banks are carrying because of the failure of some customers to secure the IT environment in which their payment processing applications and interfaces sit and to what extent banks want to try and drive customer behavior.

PT: As the nature of cyber threats continues to evolve, community initiatives are playing an increasingly important role in bolstering defenses across the industry. As a member-owned cooperative, SWIFT is working with its users to ensure that they adopt security controls as part of their business as usual processes. This is being achieved via the Customer Security Programme, which includes initiatives such as sharing intelligence on the modus operandi used in known attacks and requiring members to attest to their level of compliance with mandatory controls.

Where regulation is concerned, it is clear that regulators are looking more closely at this topic as additional threats emerge. New regulation could certainly be introduced as a result.

AT: *How will the growing shift toward instant payments impact financial crime control processes? Is it realistic for banks to run effective sanctions screening and AML monitoring programs when payments can move in seconds?*

TK: This is a huge challenge for banks. Gone are the days where a luxury of time was afforded by three- to five-day payment processing procedures.

Fortunately, RegTech solutions and other due diligence tools are being developed that can allow real-time screening to occur. But the reality is that with greater speed and efficiency of payment processing

comes a greater risk that bad actors can structure payments in such a way that automated systems fail to recognize them. This is where the rapid evolution of RegTech solutions must play a key role through the use of artificial intelligence and machine learning.

I do not advocate that machines can entirely replace humans. Humans will play a critical role in directing and fine-tuning artificial intelligence-based solutions. However, if banks are to keep up with the pace that consumers and regulators demand, then there will need to be a step change in the use of technology in order to maintain the integrity of the financial system.

AT: *In your opinion, what is the single most important key to financial crime compliance success in 2018?*

TK: Partnership and collaboration. All the technology, headcount and analysis in the world will not overcome the financial crime challenge we face if compartmentalized thinking is allowed to prevail. RUSI's Future of Financial Intelligence Sharing program precisely seeks to analyze and promote an evidence-based case for such partnership.

While technology is a key component of the development of successful partnerships, tech solutions are only as good as the information they exploit and this information can be significantly more effective if it is informed by partnership. We need more partnerships like JMLIT in the U.K., the Fintel Alliance in Australia and the Fraud and Money Laundering Intelligence Taskforce in Hong Kong, and we need these partnerships to progressively connect across borders.


The criminal elements that we seek to identify and disrupt do not respect borders—they benefit from the lack of domestic and international cooperation. The financial and law enforcement communities need to act with similar effectiveness and efficiency if they are to have a material impact on financial crime.

DF: I agree that collaboration is essential going forward. One of the biggest changes we've seen in the last couple of years has been the extent to which we are now focusing on disrupting financial crime activity, rather than simply monitoring it and telling people to protect themselves.

This can't happen in isolation. Governments, national security structures, law enforcement and technology providers are cooperating in order to identify patterns of malicious activity, which are dependent on a particular infrastructure, and actively disrupt that activity by taking down servers or shutting down accounts very quickly. This isn't just about blocking transactions and cash outs, it is about breaking down and disrupting the infrastructure used by the criminal groups themselves. And that's a team sport.

PT: Working together to tackle financial crime has never been more critical. As the threats continue to evolve and grow, banks need to collaborate with each other, with regulators, authorities and industry bodies, including SWIFT, to develop more standardized ways of working.

We are already seeing considerable progress. A great example is the work being carried out by the Wolfsberg Group, which revised its Due Diligence Questionnaire for Correspondent Banks in order to reflect changed and enhanced regulatory requirements.

With a growing focus on cybersecurity, it is likely that we will see further regulatory developments in this area. As this happens, we hope that the industry and regulators will work together effectively in order to build a standardized approach, thereby avoiding the type of fragmented regulatory environment that exists in other areas of financial crime. 

Interviewed by: Jeffrey Schenck, marketing communications manager, SWIFT, Brussels, Belgium, jeffrey.schenck@swift.com