Monday, July 13, 2020

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

In *traditional identity payments fraud*, a fraudster pretends to be another real person and uses his or her credit. The victim is directly affected financially, so this type of fraud is typically detected and reported relatively quickly.

In *synthetic identity payments fraud*, a fraudster creates a new identity to commit fraud in one of several ways. Methods include *identity fabrication* (a completely fictitious identity without any real PII), *identity manipulation* (using slightly modified real PII to create a new identity), or *identity compilation* (a combination of real and fake PII, such as a false driver's license, to form a new identity).

The Federal Reserve has published a new paper with title *Mitigating Synthetic Identity Fraud in the U.S. Payment System*. It is highly recommended to read it.

Synthetic identity accounts behave more like normal customers – building credit over a period of time – than *conventional* identity fraudsters, who must rapidly cash in before the victim notices and reports the theft.

Organizations that have the most success are those that look beyond basic PII elements (such as name, SSN, date of birth and address) and use additional data sources to gain reasonable assurance of the applicant's identity.

There are benefits to use robust *link analysis processes* – processes that look across various banking instruments (such as checking accounts, lending accounts and other financial instruments) to identify relationships or common characteristics of synthetic identities.

Examples include screening for multiple account applications originating from the same IP address or device and detecting potential fraud networks by linking identities that appear as authorized users on multiple accounts.

Link analysis also can be conducted across multiple banks from service providers that have multiple financial institutions as clients. We see increased use of *artificial intelligence (AI) and machine learning* – the use of technology to perform tasks that normally require human intelligence – to detect and mitigate synthetic identity fraud.

While the technological capabilities of these models are developing rapidly, the industry must collect more and better data in order for these AI and machine learning solutions to improve their sensitivity and more successfully mitigate fraud.

There is no single solution to completely mitigate synthetic identity payments fraud. Factors such as the regulatory environment, technological advancement and shifts in fraudster tactics create a constantly evolving payments fraud landscape.

Information sharing within – and between – organizations can help the industry draw connections between datasets to better identify potential synthetic identities.

Read more at number 8 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 5)

BIS, Annual Report 2019/20

Number 2 (Page 7)

Conclusions from the FSB's too-big-to-fail evaluation

Number 3 (Page 11)

EIOPA's response to the European Commission's Digital Finance Strategy consultation

Number 4 (Page 14)

Sound management of risks related to money laundering and financing of terrorism, January 2014 (rev. July 2020)

Number 5 (Page 16)

NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation

Number 6 (Page 20)

ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme

The EUCC Candidate Scheme for ICT Products, set to replace the SOG-IS, is released today for public feedback.

Number 7 (Page 22)

FSB statement on the impact of COVID-19 on global benchmark reform

Number 8 (Page 24)

Mitigating Synthetic Identity Fraud in the U.S. Payment System

Number 9 (Page 27)

EINSTEIN Data Trends – 30-day Lookback

Number 10 (Page 29)

Face Coverings Made From Layered Cotton Fabric Likely Slow the Spread of COVID-19 Better Than Synthetics

Number 1

BIS, Annual Report 2019/20

BIS 1930 2020 Promoting monetary and financial stability

Looking forward and back

In 2019/20, we continued to shape the Bank for the future with our Innovation BIS 2025 strategy while remembering our origins as we prepared to commemorate our 90th anniversary in 2020.

This has given us an opportunity to reflect on our role and how it has evolved over the years, while staying true to our mission to serve central banks in their pursuit of monetary and financial stability, and being ready to adapt to new challenges in a dynamic and changing external environment.

Innovation BIS 2025 is our medium-term strategy.

Launched in early 2019, it comprises a set of initiatives that position the Bank for the challenges ahead.

It aims to build a stronger BIS that embraces continuous innovation on both the analytical and business fronts, at the same time as it considers best practices at the organisation-wide level.

The Innovation BIS 2025 strategy reflects how innovation and technology are reshaping the financial landscape and the way we work, to help us meet the challenges of the digital age.

Under the strategy, we are investing in next-generation technology to build a resilient and future-ready digital workplace across the Bank.

Innovation BIS 2025 consists of a set of initiatives anchored by our mission: to serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas, and to act as a bank for central banks.

We broadened our economic analysis and research to include new themes.

We made particular progress in our work on the impact of technological innovation and monetary policy frameworks, reflected in BIS and external publications and statistics.

We also enhanced our other analytical output, especially that related to the impact of Covid-19 on the economy.

There was also a full programme of conferences and research network events.

To read more (206 pages) you may visit:
https://www.bis.org/about/areport/areport2020.pdf

The CBDC pyramid: from consumer needs to design choices

Number 2

Conclusions from the FSB's too-big-to-fail evaluation

Claudia M. Buch, Vice-President, Deutsche Bundesbank sets out the conclusions from the FSB's evaluation of the effects of too-big-to-fail reforms.

The report finds that too-big-to-fail reforms made banks more resilient and resolvable, but gaps need to be addressed.

Responses to the public consultation are invited by 30 September 2020.

Conclusions from the FSB's too-big-to-fail evaluation

You may visit:
https://www.youtube.com/watch?v=bwzQo88w8AM&feature=youtu.be

FSB FINANCIAL STABILITY BOARD

Evaluation of the effects of too-big-to-fail reforms

Consultation Report

This consultation report presents the preliminary results of, and seeks comments on, the evaluation on the effects of too-big-to-fail (TBTF) reforms for systemically important banks.

The TBTF reforms being evaluated have three components:

(i) standards for additional loss absorbency through capital surcharges and total loss-absorbing capacity requirements;

(ii) recommendations for enhanced supervision and heightened supervisory expectations; and

(iii) policies to put in place effective resolution regimes and resolution planning to improve the resolvability of banks.

These reforms were endorsed by the G20 in the aftermath of the 2007-08 global financial crisis and have been implemented in FSB jurisdictions over the course of the past decade.

The objective of this evaluation is to examine the extent to which the reforms are reducing the systemic and moral hazard risks associated with systemically important banks, as well as their broader effects on the financial system.

This report is being released in the midst of the unprecedented and still-evolving COVID-19 pandemic.

The pandemic represents the biggest test of the post-reform financial system to date, as it has pushed the global economy into a recession of uncertain magnitude and duration.

The rapid and coordinated response by fiscal, financial and monetary authorities has mitigated the impact of the shock on the real economy and the financial system.

Authorities are making use of the flexibility built into existing international standards – including bank-specific and macroprudential buffers – to sustain the supply of financing to the real economy.

However, the effects of the pandemic continue to put the financial system under strain.

This evaluation has not examined the implications of recent economic and financial developments because the analysis in the consultation report was largely completed before the outbreak of the pandemic.

The report does not look at specific banks, nor does it make policy proposals.

Nevertheless, it draws a number of conclusions that are relevant to policymakers, market participants and other stakeholders in the current situation.

The findings of the report suggest that TBTF reforms have contributed to the resilience of the banking sector and its ability to absorb, rather than amplify, shocks.

Major banks are much better capitalised, less leveraged and more liquid than they were before the global financial crisis.

Systemically important banks in advanced economies have built up significant loss-absorbing and recapitalisation capacity by issuing instruments that can bear losses in the event of resolution.

A key finding of the report is that significant progress has been made since the global financial crisis in establishing resolution regimes and enhancing the resolvability of banks.

These reforms give authorities more options for dealing with banks in distress, though which options are used is for individual authorities to consider in light of the particular circumstances.

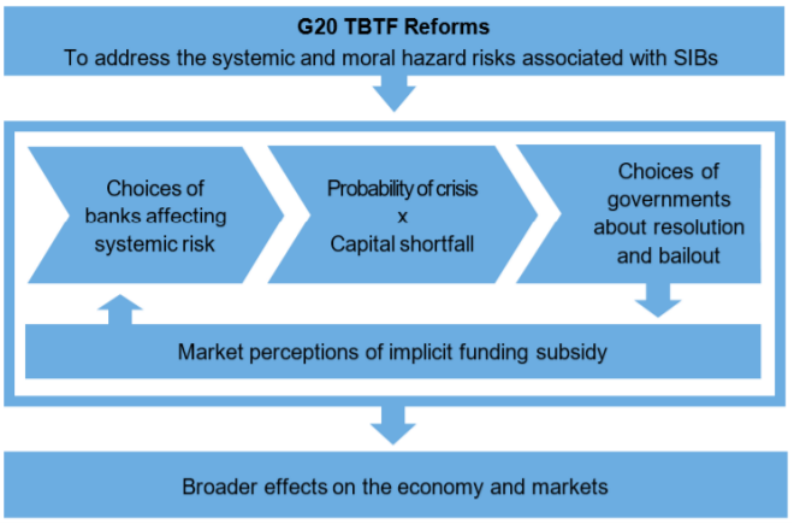
Resolution planning, together with enhanced supervision, have significantly improved the operational capabilities of banks and authorities, as well as the accuracy and detail of the information available to them.

Feedback on the analysis and findings of the consultation report would be welcome, including on any additional evidence to consider and on updates to the analytical work that it may be useful to undertake in response to the pandemic.

The consultation period has been extended to the end of September in order to give respondents more time to provide feedback, and the final report is expected to be published in early 2021.

You may visit:
https://www.fsb.org/wp-content/uploads/P280620-1.pdf

Overview of the building blocks of the evaluation of too-big-to-fail reforms Figure 1



Source: FSB

Number 3

EIOPA's response to the European Commission's Digital Finance Strategy consultation

Question 1 – What are the main obstacles to fully reap the opportunities of innovative technologies in the European financial sector?

EIOPA considers that a sound approach to financial innovation should strike a balance between enhancing financial innovation and ensuring well-functioning consumer protection and financial stability frameworks.

A level playing field and technological neutrality are crucial.

To achieve this it is important to remove legislative barriers to financial innovation while guaranteeing that other objectives such as financial soundness of the insurance market, consumer protection and financial stability are not undermined.

EIOPA would like to underline that in our view, digitalisation offers significant opportunities to take the single market further forward while allowing for more efficient supervision and new products and services that offer increased value propositions and allow for greater transparency and greater market competition.

It is important to take this opportunity to set out longer term as well as shorter term targets.

In doing so, it is also important to address the risks arising from digital technologies, such as the risk of unfair treatment of consumers or related to the lack of explainability of opaque AI algorithms if there are no adequate governance measures in place.

The issue of third parties management is also particularly relevant in the digital domain, as well as the risks arising from an inadequate management of conflicts of interests/cross-selling by digital platforms.

Furthermore, from a prudential perspective the increase in digitalisation might also lead to an increase in interconnectedness, which could render extreme cyber risks more plausible and more impactful for insurance undertakings and for the economy at large.

The Covid-19 outbreak has accelerated the trend towards digital transformation of business models and shown how digital technologies can promote financial inclusion by helping address the challenges arising from social distancing measures.

On the other hand, Covid-19 outbreak has also revealed that there are groups of vulnerable consumers (e.g. low income or elderly populations) which cannot easily access digital technologies or the Internet and should therefore be protected.

It also opened the door to an increase number of cyber-attacks.

EIOPA would like to highlight three areas (more detail on these and other issues are further developed in the relevant questions in the consultation):

1. Areas where improvements or clarifications in insurance legislation could be introduced:

EIOPA considers that insurance legislation should be fit for purpose and for this reason, it is crucial to understand shifting risks and opportunities of new technologies and business models.

In this regard, improvements and clarifications could be introduced, e.g. for paper requirements by default, on the definition of insurance and on outsourcing requirements. Further refinements to address the emergence of so-called platforms may also be needed.

2. Unlocking the use of new technologies while ensuring a fair, ethical and transparent use of data:

Data is a key driver of financial innovations such as those enabled by artificial intelligence; an ethical and trustworthy data analytics governance framework is crucial, yet stakeholders have called for more guidance.

EIOPA is working with stakeholders to bring further clarity on fairness, explainability, and governance of AI algorithms through an Expert Group on Digital Ethics in insurance (GDE) drawn from a wide range of stakeholders.

3. Access to relevant datasets:

Access to data is of outmost importance for the insurance sector. In this context EIOPA would highlight the following:

3a. Open Finance/Open Insurance: EIOPA has recently started a broader discussion with different stakeholders on possible balanced, forward looking and secure approaches to Open Insurance and its risks and benefits to the insurance industry, consumers and supervisors.

This work is currently on-going, and therefore the preliminary potential risks and benefits identified should be treated cautiously. However EIOPA considers that there might be potential for the sector and its supervision if handled right.

3b. Internet of Things (IoT) data: EIOPA encourages the European Commission to promote the interoperability of applications and portability of data between different platforms (i.e. reduce lock-in effects), improve the power of consumers to switch between providers and therefore create an appropriate framework for innovation in insurance.

3c. Cyber incident reporting data: a common incident reporting framework is critical for sharing knowledge about incidents and to encourage the development and growth of sound underwriting practices. o

3d. Data standardisation: EIOPA believes it is critical that future standardisation is built on what has already been achieved. EIOPA has already extensive experience in this regard.

We are ready to be closely involved in future discussions on data standardisation. Innovation and digitalisation could also benefit from a wider adoption of existing standards (e.g. LEI).

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/submissions/eiopa-response-to-digital-finance-strategy-consultation.pdf

Number 4

Sound management of risks related to money laundering and financing of terrorism, January 2014 (rev. July 2020)

BIS

I. Introduction

1. Being aware of the risks incurred by banks of being used, intentionally or unintentionally, for criminal activities, the Basel Committee on Banking Supervision is issuing these guidelines to describe how banks should include money laundering (ML) and financing of terrorism (FT) risks within their overall risk management.

2. The Committee has a long-standing commitment to promote the implementation of sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures that are critical in protecting the safety and soundness of banks and the integrity of the international financial system. Following an initial statement in 1988, it has published several documents in support of this commitment.

In September 2012, the Committee reaffirmed its stance by publishing the revised version of the Core principles for effective banking supervision, in which a dedicated principle (BCP 29) deals with the abuse of financial services.

3. The Committee supports the adoption of the standards issued by the Financial Action Task Force (FATF).

In February 2012, the FATF released a revised version of the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (the FATF standards), to which the Committee provided input.

In March 2013, the FATF also issued Financial Inclusion Guidance, which has also been considered by the Committee in drafting these guidelines.

The Committee's intention in issuing this paper is to support national implementation of the FATF standards by exploring complementary areas and leveraging the expertise of both organisations.

These guidelines embody both the FATF standards and the Basel Core Principles for banks operating across borders and fits into the overall framework of banking supervision.

Therefore, these guidelines are intended to be consistent with and to supplement the goals and objectives of the FATF standards, and in no way should they be interpreted as modifying the FATF standards, either by strengthening or weakening them.

4. In some instances, the Committee has included cross-references to FATF standards in this document in order to assist banks in complying with national requirements based on the implementation of those standards.

However, as the Committee's intention is not to simply duplicate the existing FATF standards, cross-references are not included as a matter of routine.

5. The Committee's commitment to combating money laundering and the financing of terrorism is fully aligned with its mandate "to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability".

To read more: https://www.bis.org/bcbs/publ/d505.pdf

Number 5

NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation

NCA
National Crime Agency

Entire organised crime groups dismantled during Operation Venetic with 746 arrests, and £54m criminal cash, 77 firearms and over two tons of drugs seized so far.

UK law enforcement has made a massive breakthrough in the fight against serious and organised crime after the takedown of a bespoke encrypted global communication service used exclusively by criminals.

EncroChat was one of the largest providers of encrypted communications and offered a secure mobile phone instant messaging service, but an international law enforcement team cracked the company's encryption.

There were 60,000 users worldwide and around 10,000 users in the UK – the sole use was for coordinating and planning the distribution of illicit commodities, money laundering and plotting to kill rival criminals.

Since 2016, the National Crime Agency has been working with international law enforcement agencies to target EncroChat and other encrypted criminal communication platforms by sharing technical expertise and intelligence.

Two months ago this collaboration resulted in partners in France and the Netherlands infiltrating the platform. The data harvested was shared via Europol.

Unbeknown to users the NCA and the police have been monitoring their every move since then under Operation Venetic – the UK law enforcement response.

Simultaneously, European law enforcement agencies have also been targeting organised crime groups.

The EncroChat servers have now been shut down.

Operation Venetic is the biggest and most significant operation of its kind in the UK.

The NCA, Regional Organised Crime Units (ROCUs) and police forces have punched huge holes in the UK organised crime network so far by arresting 746 suspects and seizing:

- Over £54million in criminal cash

- 77 firearms, including an AK47 assault rifle, sub machine guns, handguns, four grenades, and over 1,800 rounds of ammunition

- More than two tonnes of Class A and B drugs

- Over 28 million Etizolam pills (street Valium) from an illicit laboratory

- 55 high value cars, and 73 luxury watches

In addition, a specialist NCA team, working closely with policing partners, has prevented rival gangs carrying out kidnappings and executions on the UK's streets by successfully mitigating over 200 threats to life.

Organised crime groups in the UK have been using EncroChat, communicating freely believing the technology made them secure. The criminal group behind EncroChat operated from outside the UK.

On 13 June EncroChat realised the platform had been penetrated and sent a message to its users urging them to throw away their handsets.

The phones – which have pre-loaded apps for instant messaging, the ability to make VOIP calls and a kill code which wipes them remotely – have no other conventional smart phone functionality and cost around £1,500 for a six-month contract.

And recent messages from some of the UK handsets included:

- "This year the police are winning."

- "NCA as u know well are sophisticated and relentless."

- "If NCA then we have a big problem."

- "The police are having a field day."

The NCA created the technology and specialist data exploitation capabilities required to process the EncroChat data, and help identify and locate offenders by analysing millions of messages and hundreds of thousands of images.

Intelligence packages were disseminated to NCA operational teams, ROCUs, Police Service of Northern Ireland, Police Scotland, Metropolitan Police, Border Force, the Prison Service, and HMRC to develop and launch investigations.

The highest-harm organised crime groups were prioritised, with officers working tirelessly to attribute the handles to real world identities.

The Crown Prosecution Service is leading all the Operation Venetic prosecutions.

NCA Director of Investigations Nikki Holland, said:

"The infiltration of this command and control communication platform for the UK's criminal marketplace is like having an inside person in every top organised crime group in the country.

"This is the broadest and deepest ever UK operation into serious organised crime.

"The NCA is proud to have led the UK part of this operation, working in partnership with policing and other agencies. The results have been outstanding but this is just the start.

"A dedicated team of over 500 NCA officers has been working on Operation Venetic night and day, and thousands more across policing. And it's all been made possible because of superb work with our international partners.

"Together we've protected the public by arresting middle-tier criminals and the kingpins, the so-called iconic untouchables who have evaded law enforcement for years, and now we have the evidence to prosecute them.

"The NCA plays a key role in international efforts to combat encrypted comms. I'd say to any criminal who uses an encrypted phone, you should be very, very worried."

National Police Chiefs' Council lead for serious organised crime, Chief Constable Steve Jupp, said:

"This unique operation has specifically focussed on those thought to be involved in the highest levels of organised crime and drugs supply across the UK.

"I want to emphasise that this work is the culmination of meticulous planning to tackle the most serious and organised crimes groups that have been working in our communities.

"Serious organised crime is complex but working together with our Regional Organised Crimes Units and the National Crime Agency we have achieved an unparalleled victory against the kingpin criminals whose criminal activity and violence intimidates and exploits the most vulnerable.

"By dismantling these groups, we have saved countless lives and protected communities across the UK.

"Every UK police force has worked together to carry out these warrants, and I'm extremely proud of their hard work and determination which doesn't stop here.

"This sort of activity is just one aspect of our continued fight to tackle serious and organised crime. I hope this sends a clear message to the public of our determination to rid communities of this sort of criminalisation."

Home Secretary Priti Patel said:

"This operation demonstrates that criminals will not get away with using encrypted devices to plot vile crimes under the radar.

"The NCA's relentless targeting of these gangs has helped to keep us all safe. I congratulate them and law enforcement partners on this significant achievement.

"I will continue working closely with the NCA and others to tackle the use of such devices – giving them the resources, powers and tools they need to keep our country safe."

Number 6

ENISA Launches Public Consultation for First Candidate Cybersecurity Certification Scheme

The EUCC Candidate Scheme for ICT Products, set to replace the SOG-IS, is released today for public feedback.

The European Union Agency for Cybersecurity, ENISA, is launching a month-long public consultation for the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC).

The scheme aims to replace the existing schemes operating under the SOG-IS MRA for ICT products, to add new elements and to extend the scope to cover all EU Member States.

The public consultation allows interested parties to provide feedback on the draft of the EUCC candidate scheme and the outcome will be processed and shared. The consultation will remain open for contributions until July 31st, 12:00 CET.

Over the past two decades, the Common Criteria have proven efficient for the certification of chips and smartcards across Europe, and have enhanced the level of security of electronic signature devices, for means of identification such as passports, banking cards and tachographs for lorries. More recently, the criteria have been used intensively to certify the cybersecurity of ICT software products.

This new candidate scheme aims to further improve the Union's internal market conditions for ICT products, and positively affects the ICT services and ICT processes relying on such products.

About the EUCC candidate scheme:

- Built on the current SOG-IS MRA and Common Criteria with rules included for transition;
- Applicable to ICT products;
- Covers assurance levels 'Substantial' and 'High';
- Certificate validity for five years, can be renewed;

- Allows for composite certification;
- Recognition in all EU Member States;
- Voluntary scheme;
- Harmonised conditions for vulnerability handling and disclosure;
- Clearly defined rules on monitoring and handling non-compliance and non-conformity;
- Introduces a new patch management mechanism to support vulnerability handling;
- Use of a framework-based label and a QR code to ensure easy access to accurate certification information.

The EU Cybersecurity Act of 2019 (CSA) lays down an EU cybersecurity certification framework for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as of avoiding fragmentation of the internal market.

ENISA's task under the CSA is to prepare and develop candidate cybersecurity certification schemes with the involvement and support of stakeholders and a working group.

The first ad hoc working group for this scheme, the EUCC AHWG, was set up late last year by ENISA, and is chaired by the Agency.

The group is composed of 20 appointed members representing industry (developers, evaluators), and 12 participants from Member States and accreditation bodies.

The EUCC AHWG has been working in close collaboration with the Commission and with the European Cybersecurity Certification Group (ECCG). The EUCC is the first candidate scheme in the framework.
A second candidate scheme is currently in preparation and relates to the certification of cloud services.

More information at:
https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes

https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

Number 7

FSB statement on the impact of COVID-19 on global benchmark reform

The Financial Stability Board (FSB) has discussed the impact of COVID-19 on global benchmark transition.

The FSB's Official Sector Steering Group (OSSG) is monitoring the developments closely and recognises that some aspects of firms' transition plans are likely to be temporarily disrupted or delayed, while others can continue.

The FSB maintains its view that financial and non-financial sector firms across all jurisdictions should continue their efforts in making wider use of risk-free rates in order to reduce reliance on IBORs where appropriate and in particular to remove remaining dependencies on LIBOR by the end of 2021.

LIBOR transition remains an essential task that will strengthen the global financial system.

COVID-19 has highlighted that the underlying markets LIBOR seeks to measure are no longer sufficiently active.

Moreover, these markets are not the main markets that banks rely upon for funding.

The increase in the most widely used LIBOR rates in March put upward pressure on the financing cost of those paying LIBOR-based rates.

For those borrowers, this offset in large part the reductions in interest rates in those jurisdictions where central banks have lowered policy rates.

Relevant national working groups are co-ordinating changes to intermediate milestones in their benchmark transition programmes, where appropriate, to ensure global coordination.

Financial and other firms should continue to ensure that their transition programmes enable them to transition to LIBOR alternatives before end-2021.
LIBOR transition is a G20 priority, and the G20 in its February 2020 communique asked the FSB to identify remaining challenges to benchmark transition by July 2020 and to explore ways to address them.

The FSB will publish a report on these issues later this month. FSB members, in collaboration with other standard-setting bodies and international institutions, will continue to monitor developments.

Notes

The FSB set out in 2014 a series of recommendations for strengthening key interbank offered rates (IBORs) in the unsecured lending markets, and for promoting the development and adoption of alternative nearly risk-free reference rates, where appropriate.

The FSB and member authorities, through the FSB Official Sector Steering Group (OSSG) chaired by Andrew Bailey (Governor, Bank of England) and John Williams (President and CEO, Federal Reserve Bank of New York), are working to implement and monitor these recommendations.

The FSB published its most recent annual progress report in December 2019 on implementation of the recommendations.

The FSB coordinates at the international level the work of national financial authorities and international standard-setting bodies and develops and promotes the implementation of effective regulatory, supervisory, and other financial sector policies in the interest of financial stability.

It brings together national authorities responsible for financial stability in 24 countries and jurisdictions, international financial institutions, sector-specific international groupings of regulators and supervisors, and committees of central bank experts.

The FSB also conducts outreach with approximately 70 other jurisdictions through its six Regional Consultative Groups.

The FSB is chaired by Randal K. Quarles, Vice Chairman, US Federal Reserve; its Vice Chair is Klaas Knot, President, De Nederlandsche Bank. The FSB Secretariat is located in Basel, Switzerland, and hosted by the Bank for International Settlements.

Number 8

Mitigating Synthetic Identity Fraud in the U.S. Payment System

In 2019, the Federal Reserve published two white papers as part of our Payments Fraud Insights series.

Our goal was to raise awareness and encourage industry action against synthetic identity fraud, reportedly the fastest-growing type of financial crime facing the United States.

The first paper focused on causes and contributing factors of synthetic identity fraud and its impact on the U.S. payment system, while the second focused on detecting synthetics and examples of sharing information across the industry.

This white paper picks up where our last one left off. It highlights different ways that organizations – both individually and collectively – can work to mitigate synthetic identity fraud.

Additionally, we summarize a number of external factors that impact mitigation, such as the regulatory environment.

Synthetic identity fraud is not a problem that any one organization or industry can tackle independently, given its far-reaching effects on the U.S. financial system, private industries – such as healthcare, automotive and insurance – government entities and consumers.

The Federal Reserve recognizes the need for collaboration as we work with a wide array of payments industry stakeholders to advance U.S. payments security, which is consistent with the approaches described in our paper, Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey.

Our Payments Fraud Insights white papers were made possible by the contributions of many industry and government subject matter experts and Federal Reserve colleagues.

We appreciate your shared insights and look forward to continued dialogue and collaboration in reducing synthetic identity payments fraud.

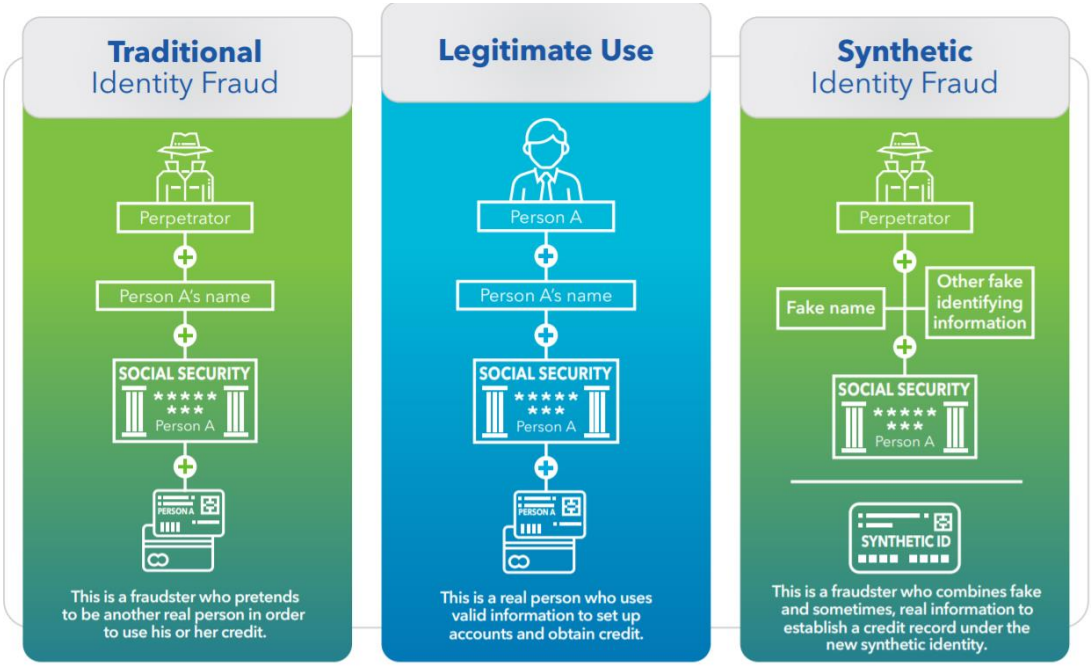
Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes, real information, such as names and Social Security numbers (SSNs), to create new identities.

These identities may then be used to defraud financial institutions, private industry, government agencies or individuals.

Differing definitions and approaches to detection make it difficult to quantify the impact on the U.S. financial system.

One widely reported analysis by Auriemma Group suggested that synthetic identity fraud cost U.S. lenders $6 billion and accounted for 20% of credit losses in 2016.

Our first white paper, Synthetic Identity Fraud in the U.S. Payment System, described key characteristics of this type of fraud. You can find it at: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf



Fraudsters leverage the personally identifiable information (PII) of individuals – frequently children, the elderly or homeless – who are less likely to access their credit information and thus, discover the fraud.

Synthetic identities can behave like legitimate accounts and may not be flagged as suspicious using conventional fraud detection models. This affords perpetrators the time to cultivate these identities, build positive credit histories, and increase their borrowing or spending power before

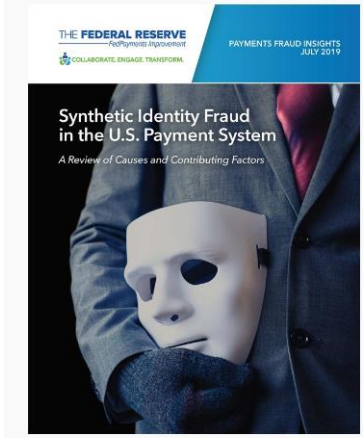
"busting out" – the process of maxing out a line of credit with no intention to repay.

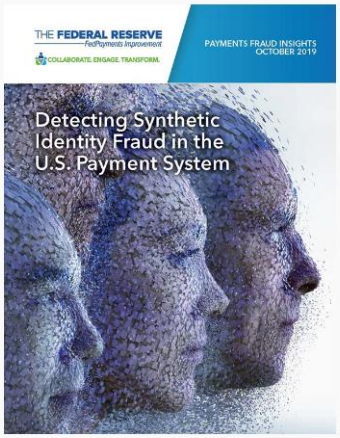
The ease and low cost of creating synthetic identities contributes to the widespread impact of this type of fraud on financial institutions, private industry, government agencies and individuals.

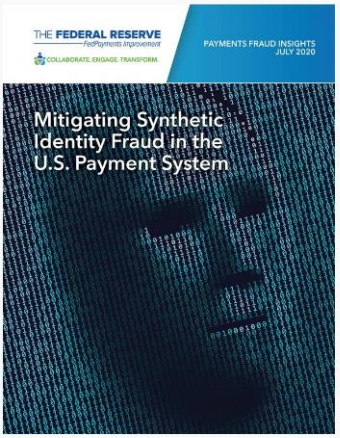
Sophisticated crime rings can leverage multiple tactics at scale to cultivate synthetic identities, including using fake addresses, creating sham businesses and forming relationships with collusive merchants to cash in.

To read more:
http://www.fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2020.pdf

https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/







Number 9

EINSTEIN Data Trends – 30-day Lookback

Cybersecurity and Infrastructure Security Agency (CISA) analysts have compiled the top detection signatures that have been the most active over the month of May in our national Intrusion Detection System (IDS), known as EINSTEIN.

This information is meant to give the reader a closer look into what analysts are seeing at the national level and provide technical details on some of the most active threats.

IDS is a network tool that uses sensors to monitor inbound and outbound traffic to search for any type of suspicious activity or known threats, alerting analysts when a specific traffic pattern matches with an associated threat.

IDS allows users to deploy signatures on these boundary sensors to look for the specific pattern, or network indicator, associated with a known threat.

The EINSTEIN Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the federal civilian departments and agencies.

By collecting information from participating federal departments and agencies, CISA builds and enhances our Nation's cyber-related situational awareness.

The signatures CISA created have been included below for analysts across various organizations to use in enhancing their own network defenses.

Note: CISA has created and tested these signatures in an environment that might not be the same for all organizations, so administrators may need to make changes or updates before using in the following signatures in their local environments.

1. NetSupport Manager RAT

The NetSupport Manager Remote Access Tool (RAT) is a legitimate program that, once installed on a victim's machine, allows remote administrative control.

In a malicious context, it can—among many other functions—be used to steal information.

Malicious RATs can be difficult to detect because they do not normally appear in lists of running programs, and they can mimic the behavior of legitimate applications.

In January 2020, Palo Alto researchers observed the abuse of NetSupport in targeted phishing email campaigns.

In November 2019, Zscaler researchers observed “software update-themed” campaigns tricking users into installing a malicious NetSupport Manager RAT.

The earliest malicious use of NetSupport was seen in a phishing email campaign—reported by FireEye researchers in April 2018.

To read more: https://www.us-cert.gov/ncas/alerts/aa20-182a

Number 10

Face Coverings Made From Layered Cotton Fabric Likely Slow the Spread of COVID-19 Better Than Synthetics

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Researchers have completed a new study of how well a variety of natural and synthetic fabrics filter particles of a similar size to the virus that causes COVID-19.

Of the 32 cloth materials tested, three of the five most effective at blocking particles were 100% cotton and had a visible raised fiber or nap, such as found on flannels.

Four of the five lowest performers were synthetic materials.

The testing also showed that multiple fabric layers could improve cotton's effectiveness even further.

None of the materials came close to the efficiency of N95 masks.

Although the sample size was relatively small, the researchers noticed that tighter woven fabrics generally filtered better than knits and loosely woven fabrics.

The 100% cotton fabrics with many raised fibers also appeared to filter better than cotton fabrics that lacked this feature.

The raised fibers often form web-like structures similar to those in medical grade masks.

Three researchers from the National Institute of Standards and Technology (NIST) — Christopher Zangmeister, James Radney and Jamie Weaver — teamed up with Edward Vicenzi of the Smithsonian Institution's Museum Conservation Institute to evaluate materials and determine both their ability to filter particles and their breathability. Their results appear in the journal ACS Nano (at https://pubs.acs.org/doi/10.1021/acsnano.0c05025).

The U.S. Centers for Disease Control and Prevention (CDC) recommends that people wear cloth face coverings in public settings (you may visit https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/diy-cloth-face-coverings.html where social distancing is difficult, primarily to prevent a person who doesn't know they're infected from spreading the virus.

The virus that causes COVID-19 is primarily spread through respiratory droplets that are expelled when a person sneezes, coughs or even talks. However, some research also suggests the virus can spread through much smaller aerosols — smaller than 1/100th the width of a human hair — that are also expelled, and which can linger in air much longer than droplets.

“It turns out that off-the-shelf materials provide some protection from aerosols if you use multiple layers of cloth and a face covering fits snugly,” said Zangmeister. “But none are as good as an N95 mask.”

The project measured a common way to determine how well a material captures particles, called filtration efficiency. Zangmeister and Radney, who are experts at measuring aerosols, set up a relatively simple experiment that relied on extremely sensitive equipment for sizing and counting aerosol particles.

The experiments used fabric samples, or swatches, rather than complete masks. “Basically, we take a swatch of material and flow a stream of particles of a known size at it,” said Zangmeister. “We count the number of particles in the air before and after it’s passed through the fabric. That tells us how effective the material is at capturing particles.”

Instead of real (and dangerous) samples of the SARS-CoV-2 virus, the team used table salt, or sodium chloride (NaCl), the recommended stand-in for virus particles by the CDC’s National Institute for Occupational Safety and Health (NIOSH), which establishes testing standards for N95 and other masks. The airflow rates used in the experiments were also from NIOSH test recommendations.

The researchers tested each material against particles ranging from 50 to 825 nanometers (nm) to chart its relative performance.

Meanwhile, Weaver, a materials chemist with a background in textiles, and Vicenzi, an expert in microscopy, studied each piece of fabric to determine its yarn count, weave and mass in the hopes of establishing a relationship between these characteristics and the fabric’s ability to filter particles.

The SARS-CoV-2 virus particles are about 110 nm in diameter. N95 masks are rigorously tested to ensure they block at least 95% of particles in this size range.

A HEPA (high-efficiency particulate air) filter such as those you might find in an air purifier blocks 99.97% of particles that are about 300 nm in size, and an even higher percentage of smaller particles.

Of the fabrics tested in the NIST study, the best-performing single fabric layer blocked 20% of particles in the size range of the virus.

While Zangmeister and Radney conducted the aerosol experiments at NIST's Gaithersburg, Maryland, campus, Weaver and Vicenzi were able to conduct their imaging work at home where they have been working since mid-March.

"We intentionally used inexpensive digital microscopes and freeware to do our part of the research from home," said Weaver. "One motivation for this was to develop imaging methods that would allow citizen scientists to better study fabrics for relatively little startup costs."

In addition to the fabrics, the team looked at materials including a HEPA filter, N95 mask, a surgical mask and even coffee filters, which have been suggested for use in homemade face coverings, for comparison. The team also tested combinations of fabrics (a cotton and a synthetic layer), which did not show increased effectiveness.

By combining imaging and aerosol measurements, the team found that some fabrics that filter the most particles are also the hardest to breathe through, and some even fail to meet health and safety recommendations for breathability.

"The texture turned out to be one of the more useful parameters to look at because we found that most of the cotton fabrics with raised threads tended to filter best," said Weaver. "Our findings suggest that a fabric's ability to filter particles is based on a complex interplay between material type, fiber and weave structures, and yarn count."

This research adds to the body of knowledge on fabrics and filtration that dates back to the 1918 flu pandemic that killed an estimated 20 to 50 million people worldwide and prompted the first research into fabric masks and their potential to protect against viruses. It also supports subsequent research suggesting that cloth filters would not be suitable for health-care settings.

But despite decades of research on the topic, the team found that a lack of standard test methods and the broad range of materials tested made it difficult to directly compare the results of previously published studies. They hope their work will provide a method for rapidly screening materials.

"We didn't know the answer when we started this project," said Zangmeister. "But the bottom line is that none of these fabrics are as good as an N95 mask. Still, cloth face coverings can help slow the spread of

coronavirus. We hope this research will help manufacturers and DIYers determine the best fabrics for the job and serve as a basis for additional research."

The team plans to begin another round of testing on a new set of materials in the near future. Weaver and Vicenzi have upgraded their imaging hardware and plan to employ more sophisticated textural analysis for the next round of fabrics.

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

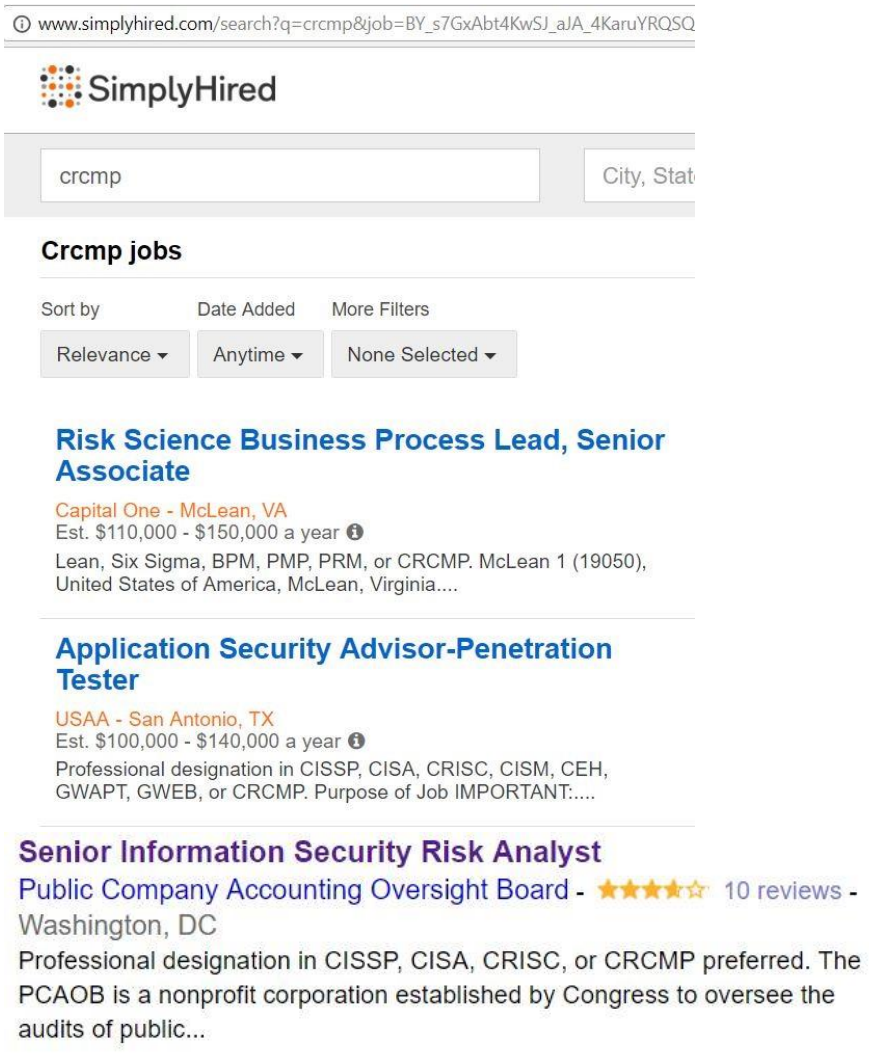
International Association of Risk and Compliance Professionals

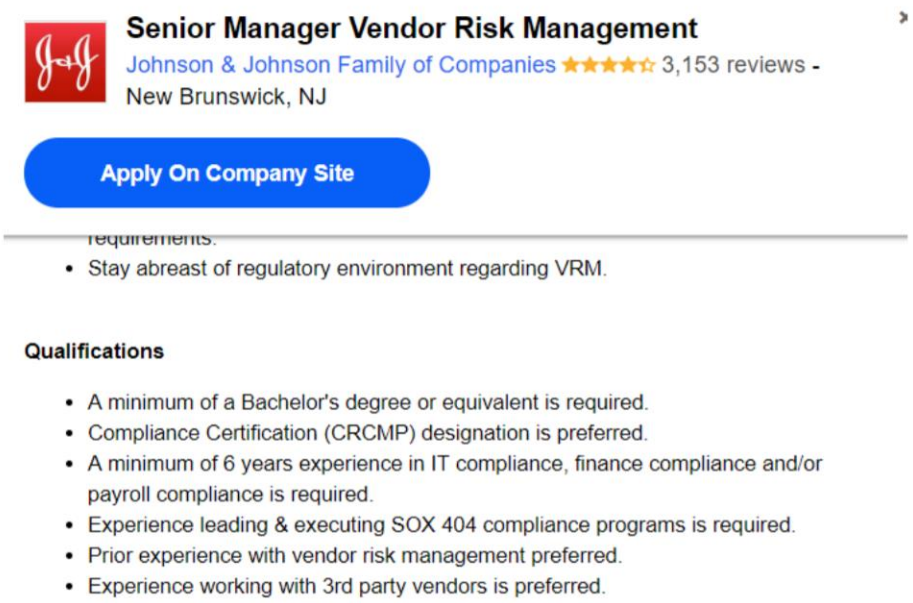
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html