EBOOK: FINANCIAL CRIME

Suspicious transaction reporting: how technology can ease the burden

BY

Nick Portalski
Chief Product Officer

Jacob Gloser
Technical Product Owner

NAPIER

About the authors

Nick Portalski

Chief Product Officer

Nick has extensive leadership experience in designing and delivering enterprise products using multiple technologies. Having worked in successful FinTech start-ups and enjoyed global responsibilities with IBM, his expertise lies in taking concepts from embryonic vision through to advanced end products.

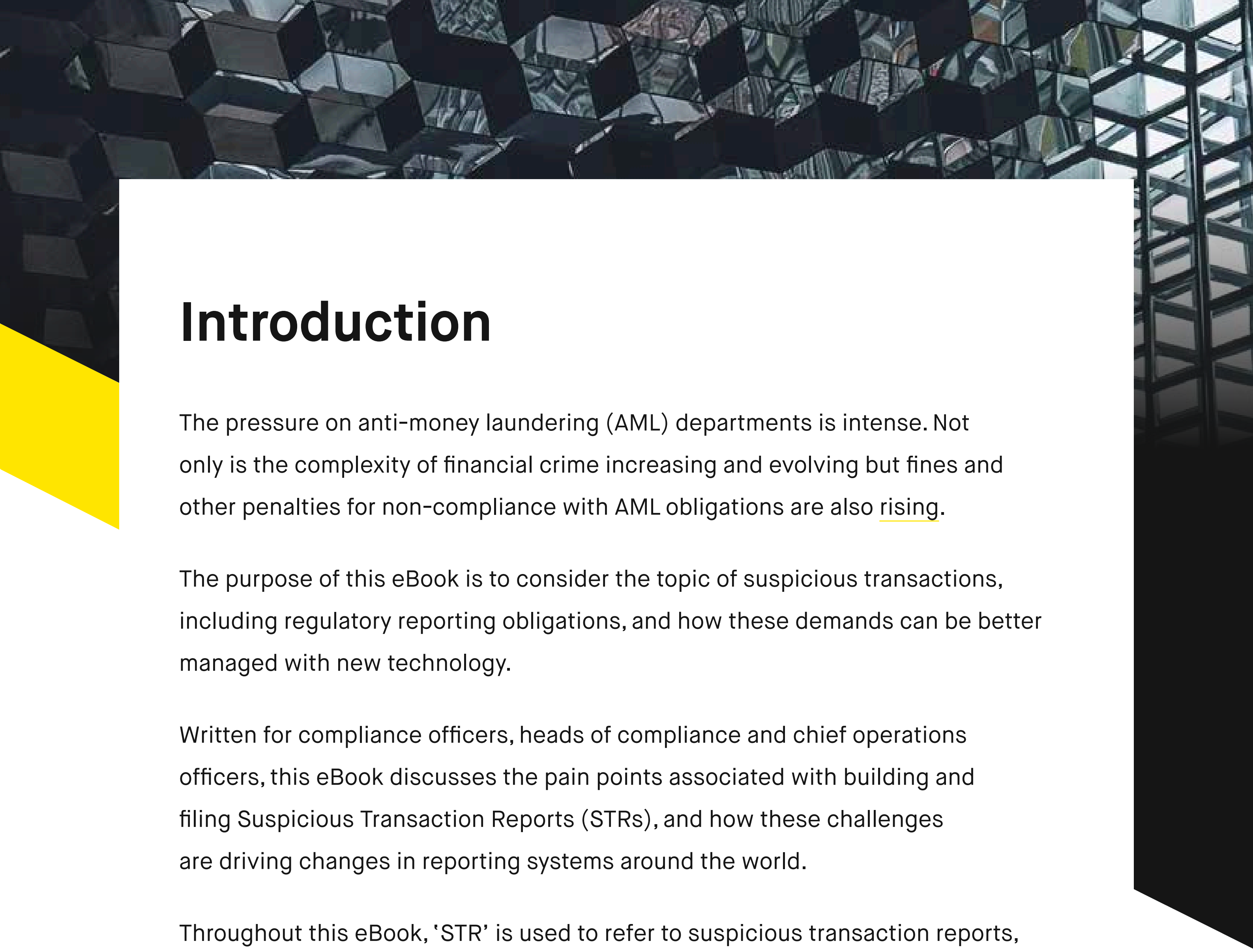
Jacob Gloser

Technical Product Owner

Jacob is a seasoned product manager with a proven track record in managing teams to create, launch and grow products and businesses. With a Chartered Financial Analyst level 1 and a passion for innovation, he brings detailed knowledge of several industries including finance and FinTech, data and research, digital products, investments and platform start-ups.

Contents

First published in 2021.



Introduction

The pressure on anti-money laundering (AML) departments is intense. Not only is the complexity of financial crime increasing and evolving but fines and other penalties for non-compliance with AML obligations are also rising.

The purpose of this eBook is to consider the topic of suspicious transactions, including regulatory reporting obligations, and how these demands can be better managed with new technology.

Written for compliance officers, heads of compliance and chief operations officers, this eBook discusses the pain points associated with building and filing Suspicious Transaction Reports (STRs), and how these challenges are driving changes in reporting systems around the world.

Throughout this eBook, 'STR' is used to refer to suspicious transaction reports, suspicious activity reports and suspicious matter reports, as the terminology varies between different parts of the world. These differences are explained in more detail on page 6.

Finally, this eBook looks at the innovative STR Builder from Napier. This new software not only dramatically reduces the time it takes to compile an STR but also provides robust data security that protects all the associated data and people.

Chapter 1: Regulatory obligations for suspicious transaction reporting

In many countries, it is a requirement by law for regulated organisations to report suspicious transactions or activity, especially those countries that are members of The Financial Action Task Force (FATF) and follow their recommendations for anti-money laundering (AML) and combating the financing of terrorism (CFT).

The United Nations categorises transactions as suspicious when there are reasonable grounds to suspect the transaction is linked to the proceeds of criminal activity or is related to terrorist financing. Suspicious activity refers to 'irregular or questionable' behaviour or activity, or a transaction that is inconsistent with normal activities or those expected for that account type.

Identifying suspicious transactions

Identifying suspicious transactions is not a straightforward process and usually relies on implementation of AML processes and systems, such as transaction monitoring, transaction screening, client screening, and regular client activity reviews.

These systems must all be run in line with regulatory guidance and follow a risk-based approach to ensure that the measures to prevent or mitigate financial risks are appropriate for the risks identified.

FATF mandates that financial institutions should be required by law to report suspicious transactions to the financial intelligence unit (FIU). To date, this has been a time and resource intensive responsibility.

Chapter 2: What is an STR?

An STR is a document that must be submitted to the relevant FIU when there are reasonable grounds to suspect an individual or organisation is laundering money, engaging in terrorist activity, or committing other financial crime.

STRs provide critical data to assist law enforcement in criminal investigations linked to all sorts of crime, from child trafficking to modern slavery, drug smuggling to terrorism. STRs play a key role in combatting money laundering and terrorist financing as they can trigger an investigation into a previously unknown criminal activity.

What's the difference between STR, SMR, and SAR?

STR is the name FATF uses for reports of suspicious activity and is the most widely used term. The term varies globally: Suspicious Activity Report (SAR) is commonly used in the UK and the USA, while Suspicious Matter Report (SMR) is preferred in Australia. STRs are also commonly referred to as 'disclosures'.

How are STRs filed?

Filing STRs has historically been a time-consuming process. Depending on the FIU, reports may be submitted in physical format and/or electronically.

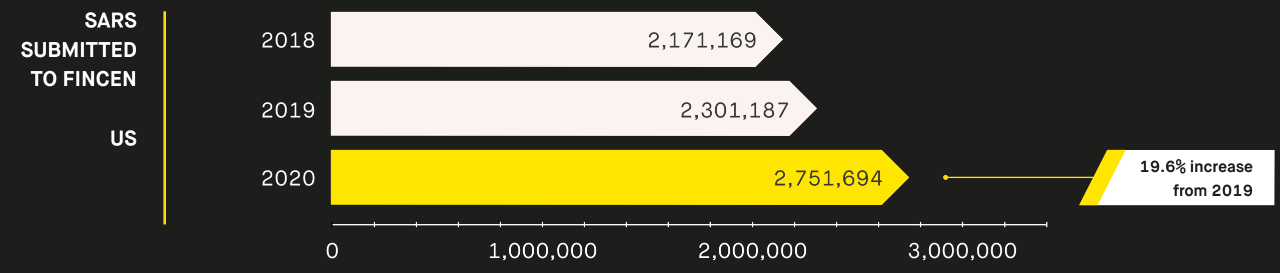
Analysts are trained to recognise, investigate, and report suspicious activity to their Money Laundering Reporting Officer (MLRO) who is responsible for submitting an STR to the FIU.

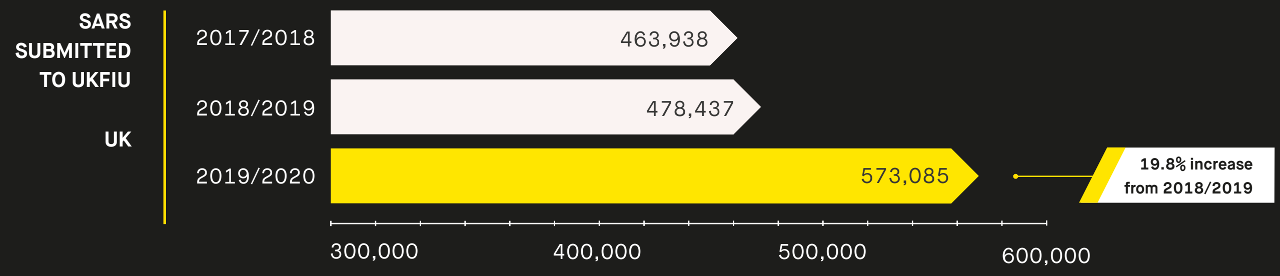
When a suspicious activity relating to money laundering or any other offence is detected, there is often a thirty day deadline to submit an STR to the FIU. That said, this deadline does vary. In Australia, the submission window is just three business days. In some cases, extensions may be permitted, depending on the complexity of the submission.

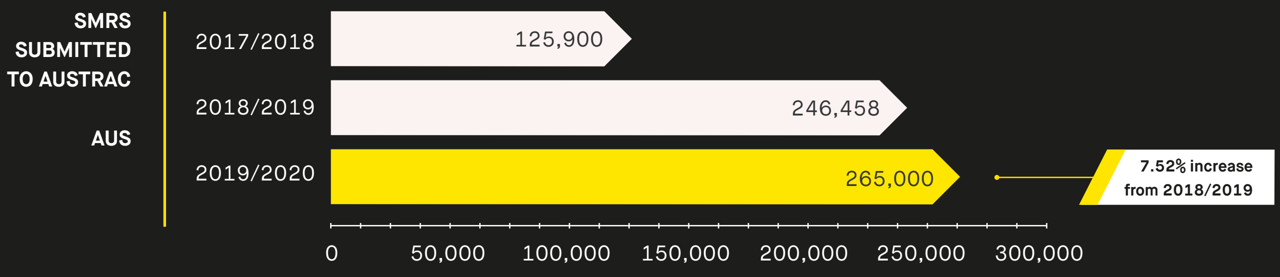
STR trends./

Worldwide, the number of STRs submitted has been increasing in recent years:

- The number of SARs filed in the US has increased by 50% since 2014 to over 2.5 million in 2020.
- Australia has seen a 258% increase in SMRs since 2016-17, relating to the submission of approximately 265,000 SMRs in 2019-20.
- Over 570,000 SARs were filed in the UK in 2020, up 20% from 2019.







While the cause of this rise is not certain, it is likely to be reflective of several factors:

1. Increasingly sophisticated AML software detecting more suspicious activity.
2. Lower risk appetite driven by increased regulatory action for reporting breaches. As the penalties for non-compliance with AML regulations have increased, so too has the number of STRs submitted. While most of these reports are likely to be justified, many banks fear being hit with penalties if an STR is not filed, so the phenomenon of defensive reporting becomes a real issue.
3. Not having enough information to safely determine whether something is suspicious or not. Organisations may deem it safer to be overly cautious and submit a report if they are unsure.
4. There is growing evidence to suggest that there has been an increase in the amount of money being laundered since 2017.

Chapter 3: Challenges in submitting STRs

Filing STRs has long been a challenging process:

1. Creating STRs can be a manual and time-consuming task

To stand the best chance of preventing and tackling crime, STRs need to be accurate and submitted within the stipulated timeframe.

For most companies this poses challenges because creating an STR is a manual, cumbersome process that requires a lot of repetitive work, including information gathering and form filling.

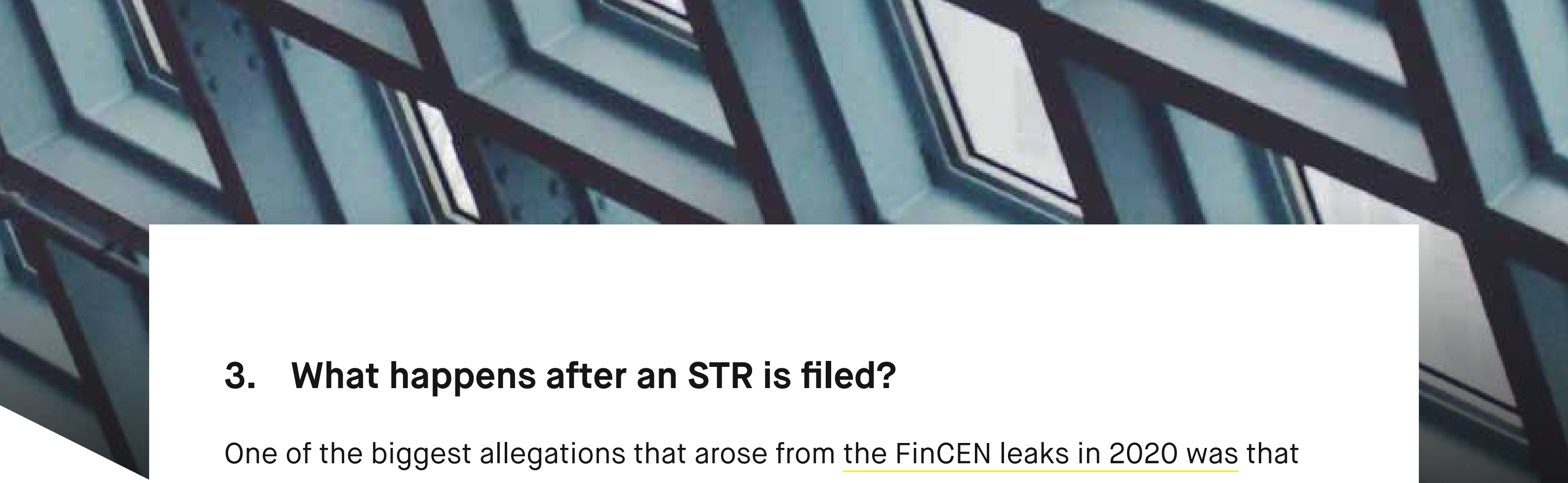
There is usually a vast amount of information that must be analysed to determine its relevance to the suspicious activity, and this can become a barrier to submission.

Since STRs are sensitive documents, there can only be a limited number of people involved in compiling one, creating a significant workload for those designated people as the work cannot be delegated or outsourced.

2. Information security must be robust

Confidentiality is paramount for ensuring the reporting process works as it is designed to and the secrecy of possible or ongoing investigations is not compromised.

FATF mandates that "financial institutions, their directors, officers and employees should be prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU."



3. What happens after an STR is filed?

One of the biggest allegations that arose from the FinCEN leaks in 2020 was that banks have not been responsible in how they deal with the subjects of STRs.

At the very least, the risk score of the subject should be recalculated following the filing of an STR against them, rather than continuing business as usual. For example, the recently discovered suspicious activity may result in a high risk score, which would subsequently demand more intensive monitoring of the subject.

Those who submit STRs are usually not provided with updates or feedback and may only become aware of its progression if law enforcement reaches out to request further information about the case.

FinCEN leaks: What happened?
More than 2,500 documents sent to US authorities between 2000 and 2017, of which the vast majority were SARs, were leaked to BuzzFeed News and shared with a group of global investigative journalists. The documents involved around $2tn of transactions and caused uproar by revealing how some of the world's biggest banks allegedly allowed criminals to launder money.

4. Maintaining an audit trail for the STR

Once STRs are submitted, the regulator can request additional information on the case for up to five years. When STRs are created manually, this can present challenges as the person who filed the STR may have moved on from the reporting entity (financial institution/company) or systems may have changed, making it difficult to retrospectively locate the data needed.

Chapter 4: How STR systems are improving around the world

The global STR landscape is gradually but positively changing in three important ways:

1. Technology is making it easier to file STRs with FIUs

New technologies are beginning to transform this otherwise time-consuming regulatory requirement.

This is because enforcement agencies around the world are introducing, allowing, and encouraging new tech, including Application Programming Interfaces (APIs), to make reporting easier.

In the US, the new Anti-Money Laundering Act has introduced several measures to make SAR filing easier, including the provision for FinCEN to "establish streamlined, including automated processes" for non-complex categories of SARs.

In response to industry demand for a better-designed SMR process, AUSTRAC has made commitments to overhaul its clunky, 20-year-old reporting system over the next four years. Almost half (44%) of reporting entities said the design was a "priority issue," so a key aim of the system update is to make the process more user-friendly, making it easier for entities to comply with their reporting obligations.

In the UK, progress is driven by Action 30 of the Government's Economic Crime Plan, which sets out to deliver SARs IT transformation. It is planned that the new digital service for SARs reporting and analysis will be completed by March 2022.

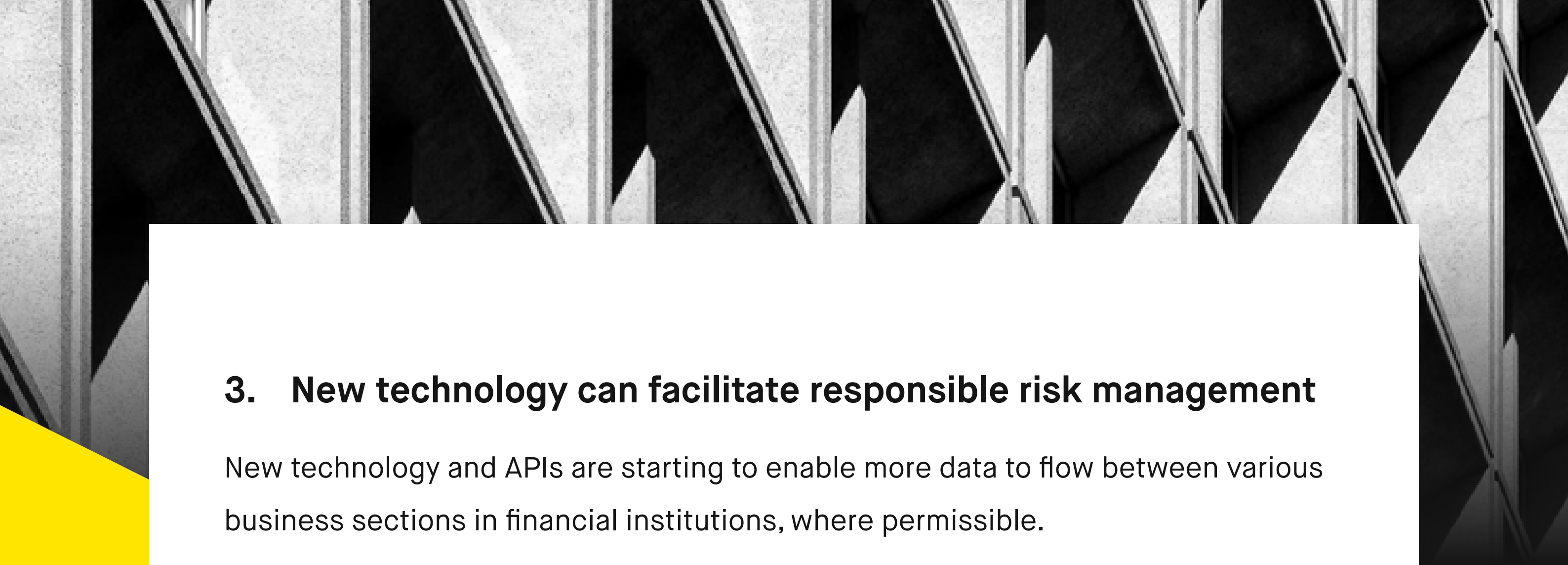
Efforts are also being focused on improving the quality of SARs submitted. Sector-specific templates, for example, are an initiative to help guide users as they submit reports and flag any errors or omissions as they occur. This is important because a significant number of SARs are of low quality and contain limited or even no useful intelligence.

2. New technology is making it easier for FIUs to process reports.

In Hong Kong, police are boosting computing power to help their new AML team cope with increasing volumes of STRs, which rose by almost 11% last year. With officers currently having to analyse STRs manually, the computer system upgrade will use big data technologies to help with STR processing, saving them time.

In the UK, the National Crime Agency's (NCA) new IT is working to better manage the volume of SARs submitted. The new tools promise to draw out the values of SARs, spotting indications of vulnerability, patterns and networks. Moreover, the new system should provide law enforcement with a better portal, including easier access and search functionality.

There is huge potential for digital automation in STR processing. This would enable automated software systems to do all the low value, repetitive work of checking STRs, so that human regulators can focus on high priority investigations.

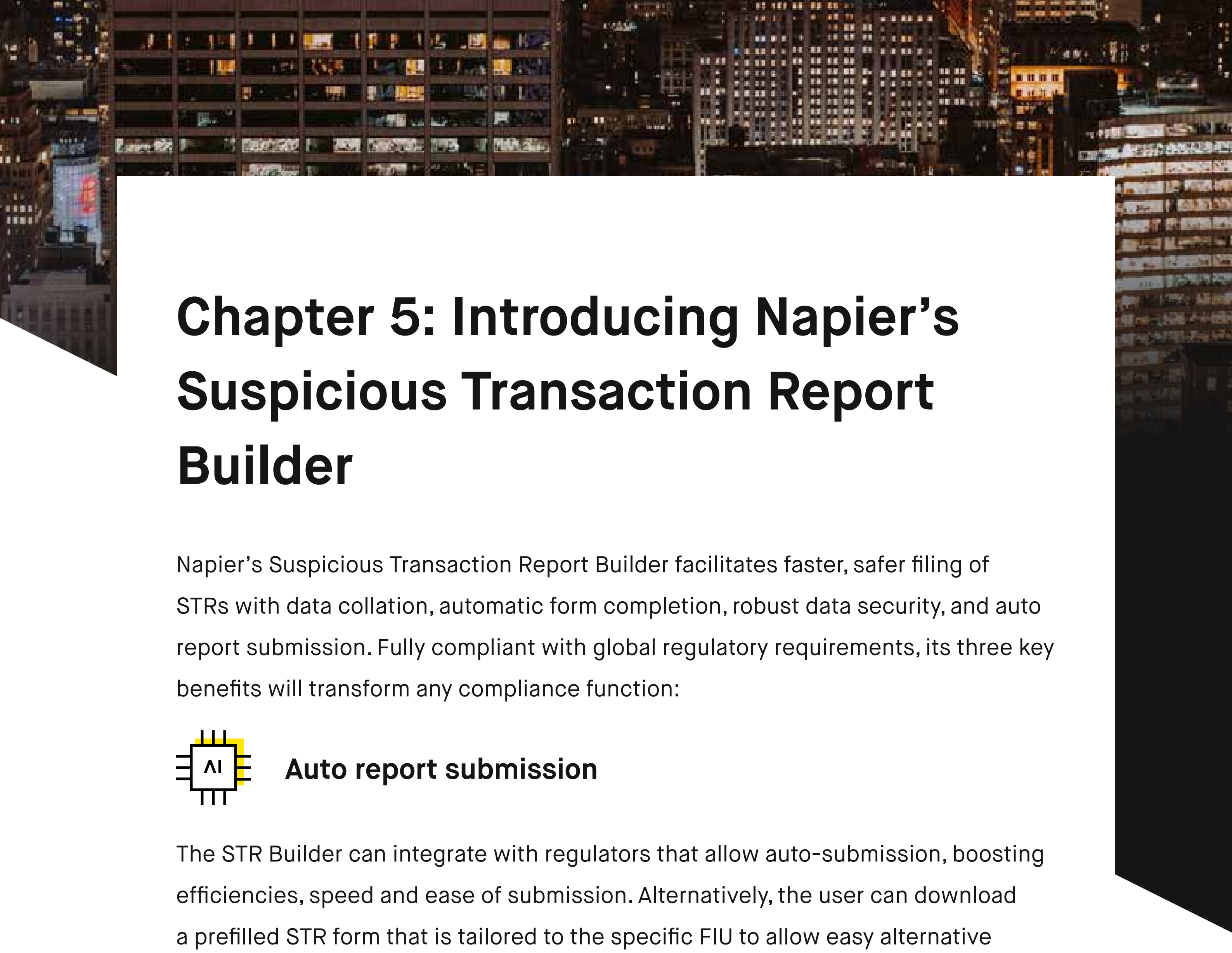


3. New technology can facilitate responsible risk management

New technology and APIs are starting to enable more data to flow between various business sections in financial institutions, where permissible.

With more data to hand, compliance teams have a greater understanding of a customer's risk level, enabling better decisions about pursuing investigations.

This approach demonstrates appropriate action to all stakeholders, rather than being perceived as continuing business as usual. Industry needs - and is beginning to see - a movement towards the continuous risk assessment of customers.



Chapter 5: Introducing Napier's Suspicious Transaction Report Builder

Napier's Suspicious Transaction Report Builder facilitates faster, safer filing of STRs with data collation, automatic form completion, robust data security, and auto report submission. Fully compliant with global regulatory requirements, its three key benefits will transform any compliance function:

Auto report submission

The STR Builder can integrate with regulators that allow auto-submission, boosting efficiencies, speed and ease of submission. Alternatively, the user can download a prefilled STR form that is tailored to the specific FIU to allow easy alternative submissions where digital submission is not possible.

Assured report security

Through encrypted form completion, Napier's STR builder ensures robust reporting security, greatly diminishing the risk of breaching tipping off regulations. STRs are encrypted and therefore not accessible to anyone but those few who have been granted specific user permissions.

Auto form completion

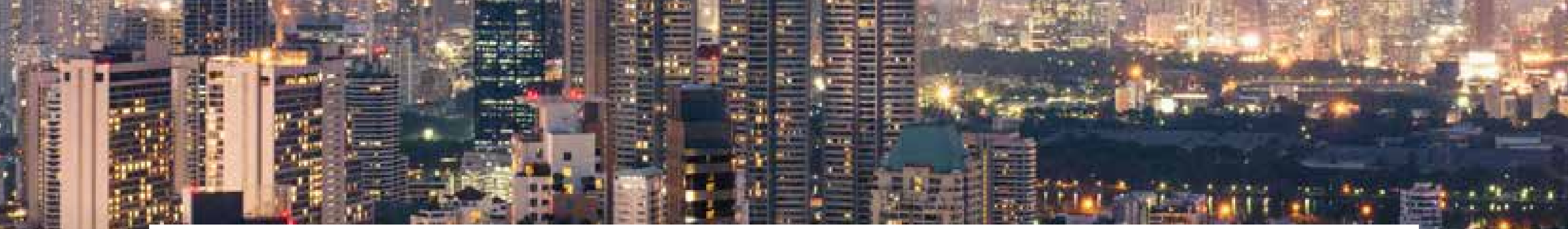
Data collection for an STR can be a time-intensive and onerous process when done manually, as the person tasked with its filing has to track down data from various sources and departments across an organisation. As this data is often siloed, getting a complete picture of the suspicious activity is difficult.

The STR Builder completes up to 80% of the form with the required information for STRs, drawing the necessary data from Napier's Transaction Monitoring system.

This submission preparation includes automatic gathering of relevant transactional data, customer data, previous notes, and attachments needed to build an audit trail and support a case.

Auto form completion greatly reduces manual input and improves the reporting process by making it faster and of a higher quality.

Once the form is complete, an informed decision can be reached on whether it will be necessary to escalate the incident and file a formal STR. Auto form completion allows human efforts to be focused on ensuring the report is of the highest quality, rather than undertaking repetitive form filling.



Final thoughts

STRs are integral to the fight against financial crime and terrorist financing. While the volume of STRs is increasing, so too are the positive real-world impacts they are facilitating, with record amounts of money now being restrained or removed from criminals.

Regulators are already showing great commitment to improving technology, and the implementation of modern technology by regulators and reporting entities can only spell improvement for AML processes and the fight against financial crime. When properly applied, technology can deliver the internal efficiencies needed to reduce the financial and human resource burdens associated with filing STRs.

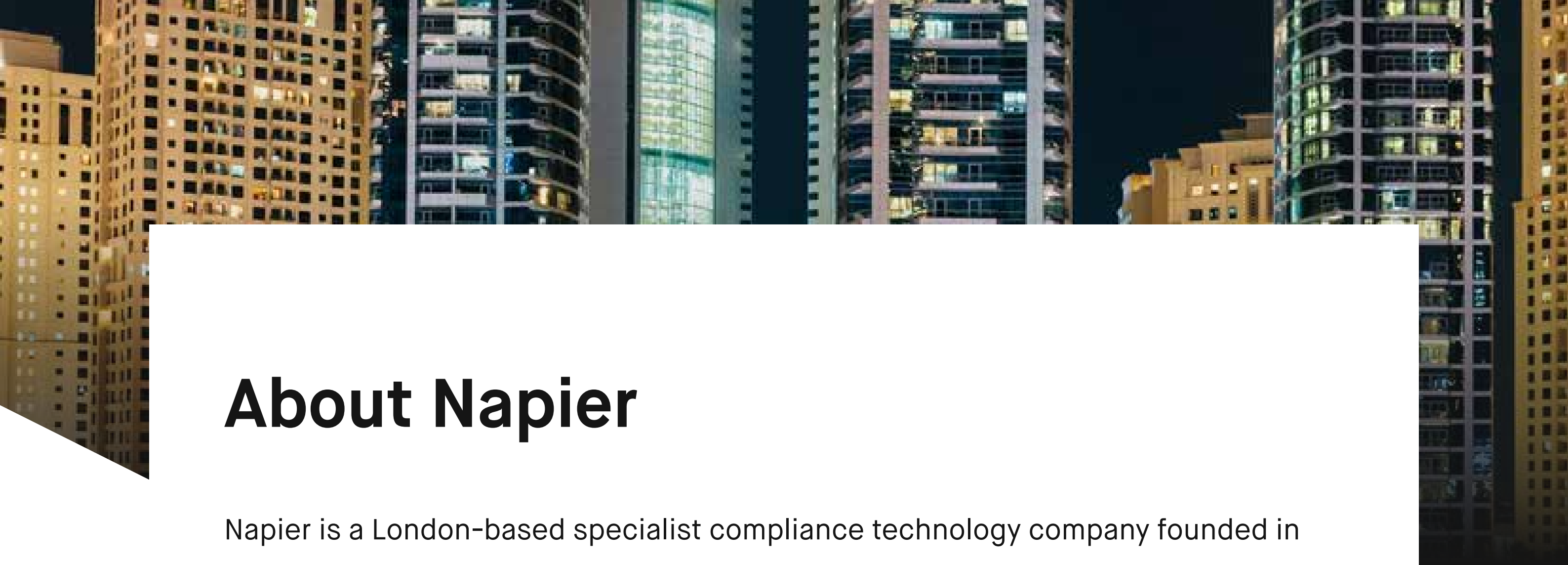
Ensuring full compliance with all STR regulatory requirements, Napier's STR Builder not only saves time but gives peace of mind with stringent data security.

By implementing Napier's STR Builder, compliance teams can focus on submitting high quality, detailed and accurate STRs, confident that the contents are secure, confidential, and compliant with anti-tipping off regulations.

Learn more about Napier's STR Builder

Napier's STR Builder is available with a separate license on purchase of one of Napier's core solutions, such as Transaction Monitoring or Transaction Screening.

To find out more, or to book a demo of the STR Builder - or any of the other solutions on our Intelligent Compliance Platform – get in touch.



About Napier

Napier is a London-based specialist compliance technology company founded in 2015 with global offices in all the key financial hubs.

Trusted by the world’s leading financial institutions, our next generation Intelligent Compliance Platform is transforming financial crime compliance.

We design and build compliance technology to help companies in any sector comply with AML regulations, detect suspicious transactions, screen potential customer and business partners, and help analysts predict customer behaviour.

Napier uses industry knowledge and cutting-edge technologies such as artificial intelligence and machine learning to help businesses detect suspicious behaviours and fight financial crime.

Discover how Napier can transform your compliance processes

Learn more about how Napier can transform your screening processes at www.napier.ai where you can book a demo or contact us.

Email us

Book a demo

NAPIER.AI