Instant Payments

Avoiding the Convergence of Complex Financial Crimes

FEATURE SPACE

OUTSMART RISK

Executive Summary

Discussions around Real-Time Payments (RTP) often include concerns that it will be accompanied by a rapid increase in financial crime. The innovation that comes with instant payment schemes is a great opportunity for a variety of reasons and preventing future financial crime will always be part of the dialog.

If you have global operations, you are likely already operating in a region where some form of real time, or instant payment scheme, is in place. Faster Payments in the UK, Fast and Secure Transfers (FAST) in Singapore and Mexico's Interbanking Electronic Payment System (SPEI) are a few examples of schemes already in operation in several countries.

In the United States, The Clearing House's Real-Time Payments platform is the first new payment system in 40 years. The Federal Reserve declared in August 2019 that they will also launch their own real-time payments rail, FedNow.

On the consumer side, Zelle® was launched in 2017 as an easy way to send money directly between almost any US bank accounts typically within minutes. In fact, it is already proven to be a success with Early Warning Services, LLC, the network operator behind Zelle, announcing that $44 billion was sent through the Zelle Network® on 171 million transactions during Q2 2019.

Most early adopters of instant payment schemes often left financial crime prevention as an afterthought.

In this paper you will find examples of some of the most prolific fraud attacks which can be fueled by instant payments. And you will find actionable recommendations for the best approaches to prevent these complex financial crimes.

Bank of International Settlements (BIS) defines instant payment systems as those in which the transmission of the payment message and the availability of 'final' funds to the payee occur in real-time or near-real-time on as near to a 24-hour and seven-day (24/7) basis as possible.

BANK FOR INTERNATIONAL SETTLEMENTS

A Positive Impact on Society

A key advantage of instant payment schemes is that it makes real-time, non-revocable payments accessible to everyone for lower value transactions. The positive effects of these schemes are demonstrated in their impact both economically and socially.

Real-Time Payments can be beneficial to society as it helps reduce crime and security issues related to cash handling. In turn this also forces criminals to legitimize money by attempting to get it into the financial system, and therefore risking exposure of any illicit activities through money laundering attempts. And it gives businesses of all sizes the ability to have greater financial control.

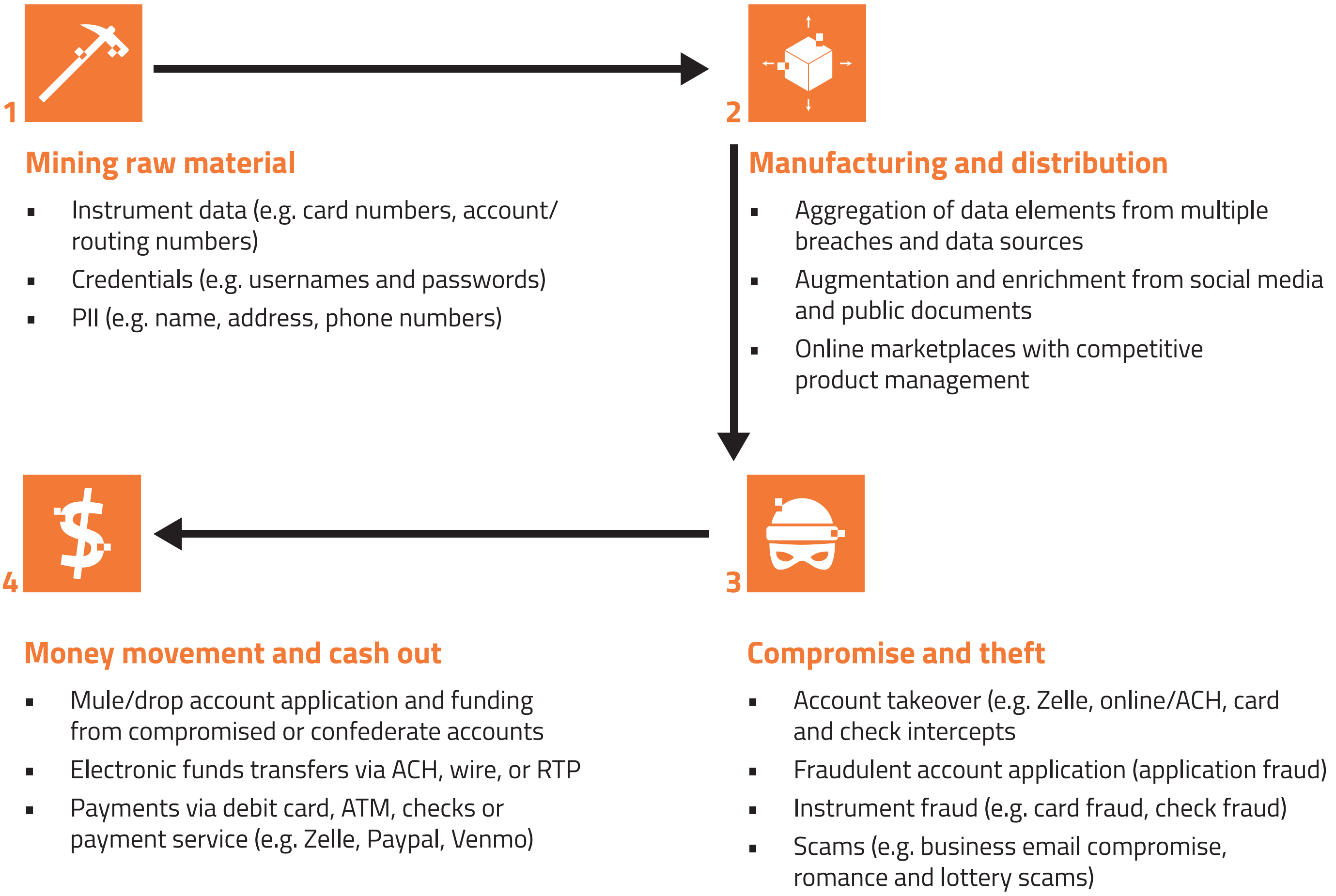
A Painful Paradigm

Before we dig deeper, it is vital to reiterate that the speed with which Real-Time Payments take place is the number one concern globally. Although a positive benefit, this is also perceived as a downside. The obvious risk trigger is that the scheme has potential to be a catalyst that could drive an increase in large amounts of fraud.

For criminals, the driving force will always be to find loopholes to legitimize financial proceeds from illicit operations, as quickly and easily as possible. A variety of examples of the types of fraud used is evident across the entire financial system, from card and payments fraud to money laundering. Policing these tactics is tough when the opportunities to exploit any weakness can come via a multitude of channels.

The Fraud Value Chain

Aite Group, in their June 2019 report entitled Trends in Account Takeover Fraud for 2019 and Beyond, uses the term Fraud Inc to describe what they call “The fraud value chain”. It is a model to describe the economics at work from the fraudster’s perspective.



1

Mining raw material

- Instrument data (e.g. card numbers, account/routing numbers)
- Credentials (e.g. usernames and passwords)
- PII (e.g. name, address, phone numbers)

2

Manufacturing and distribution

- Aggregation of data elements from multiple breaches and data sources
- Augmentation and enrichment from social media and public documents
- Online marketplaces with competitive product management

3

Compromise and theft

- Account takeover (e.g. Zelle, online/ACH, card and check intercepts
- Fraudulent account application (application fraud)
- Instrument fraud (e.g. card fraud, check fraud)
- Scams (e.g. business email compromise, romance and lottery scams)

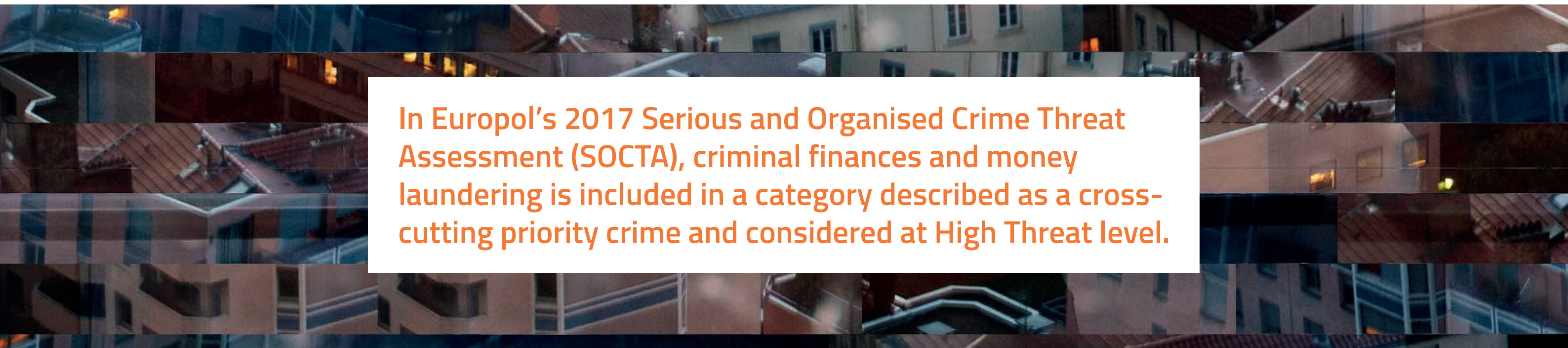
4

Money movement and cash out

- Mule/drop account application and funding from compromised or confederate accounts
- Electronic funds transfers via ACH, wire, or RTP
- Payments via debit card, ATM, checks or payment service (e.g. Zelle, Paypal, Venmo)

Debit card fraud losses (signature, PIN, and ATM combined) made up 44% or $1.2bil of losses in 2018.

American Bankers Association’s 2019 Deposit Account Fraud Survey



In Europol’s 2017 Serious and Organised Crime Threat Assessment (SOCTA), criminal finances and money laundering is included in a category described as a cross-cutting priority crime and considered at High Threat level.

Convergence of Complex Financial Crimes

The initial attack is what most financial institutions think of when combatting Real-Time Payment fraud.

It is useful to think of Real-Time Payment fraud in two distinct categories.

1. **Controlling the account and transferring the funds**
2. **Receiving the funds and cleaning the money**

Controlling the Account and Transferring the Funds

Account Takeovers (ATO)

Account Takeovers are already widespread. In the United States, ATOs reached a four year high in 2017, recording $5.1 billion in losses. Mobile phone account takeovers have proven particularly vulnerable doubling from 380,000 in 2017 to 679,000 attacks in 2018*.

In addition, data breaches have made personally identifiable information (PII) cheap and easy to get hold of. Criminals are simply making a logical business decision as they migrate from card fraud to ATOs because it is much more profitable.

In countries where instants payment schemes are already in operation, there has been an initial surge in ATOs. Consequently, it is important for banks to be vigilant as schemes are rolled out more globally.

Authorized Push Payment Scams (APP)

More adept criminals, with a flair for social engineering, will unleash various scams to cash in on Real-Time Payments. The fraudster simply pivots the attack from taking over the account and transferring the money out, to convincing the actual customer to execute the transfer.

An Authorized Push Payment (APP) scam, in its most basic form, uses social engineering to convince a customer to send money to an account which the criminal controls.

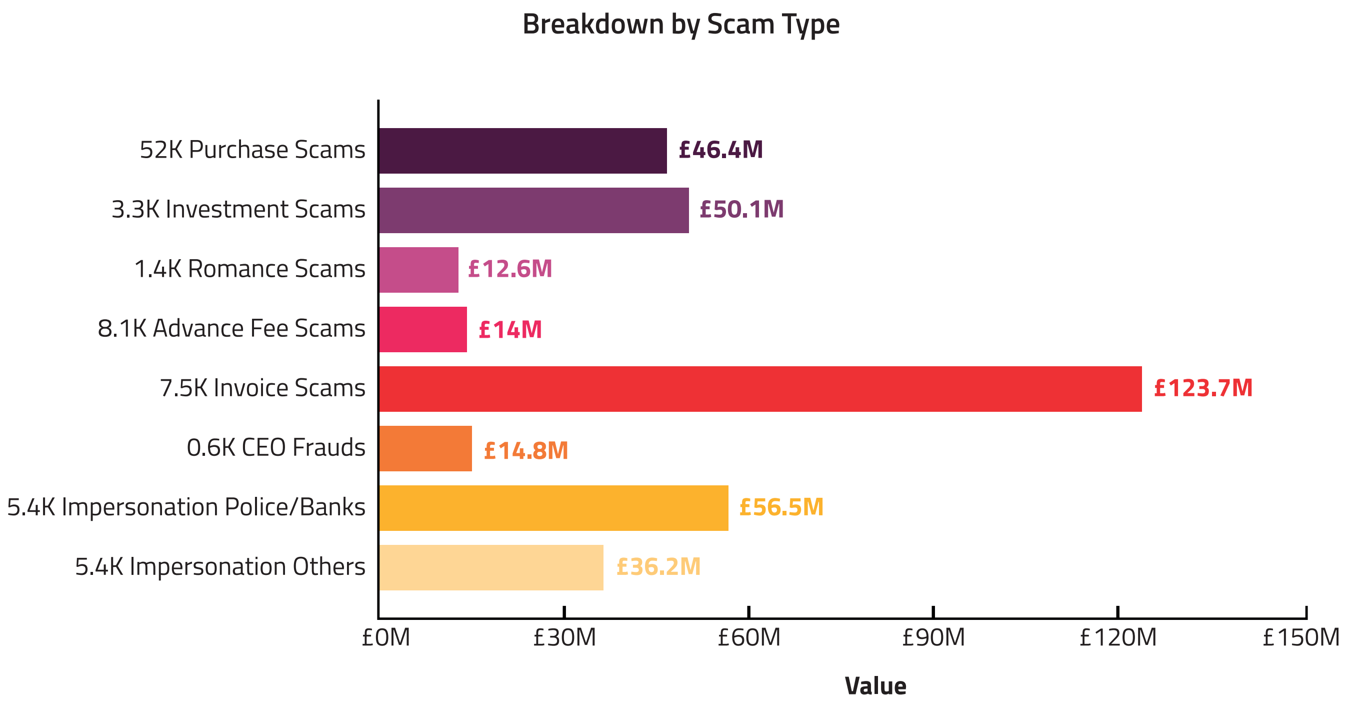
Faster Payments in the UK has been in operation for over a decade. In 2018, the UK lost £345 million to APP scams, of which only £83 million was recovered. If you look at financial crime, APP scams represented over a quarter of total losses in the UK in 2018. According to data released by banking body UK Finance, APP scams have risen by 40% in 2019 with £616m stolen using these tactics.

*Javelin 2019 Identity Fraud Study

By mid-year 2019, most large banks had already launched Zelle.

Trends in Account Takeover Fraud for 2019 and Beyond, Aite Group

The following information provides a more detailed breakdown of different scams, how they are executed and the associated data around costs and volume[†].



Purchase scam - Victim is scammed into paying for goods that they never receive.

Investment scam - Victim is scammed into investing money in a fake investment such as property and land.

Romance scam - Victim is scammed into paying funds to a person they have met through online dating websites. Fraudsters creates fake profiles to build a relationship with the victim.

Advance fee scam - Victim is scammed into making a payment for a fee which will release a higher value payment. One example could be an overseas lottery.

Invoice & Mandate scam - Victim attempts to pay a legitimate payee but the fraudster intervenes to make the victim send funds to an account they control. Usually the fraudster would have access to the victim's email account so they can pose as a known 3rd party.

CEO Fraud - The fraudsters impersonate a CEO of a company and requests the victim to make a payment to an account they control. Finance teams are often targeted with these types of scams.

Impersonation: Police/Bank Staff - The fraudster poses as the police or bank staff and request the victim send money to an account they control. The fraudster will often tell the victim that their account is at risk.

[†] UK Finance Fraud the Facts 2019

Receiving the Funds and Cleaning the Money

Banks are fighting highly motivated criminals who have access to unlimited resources to meet their end goal. The following are examples of the more frequently seen tactics used by criminals for legitimizing illicit gains.

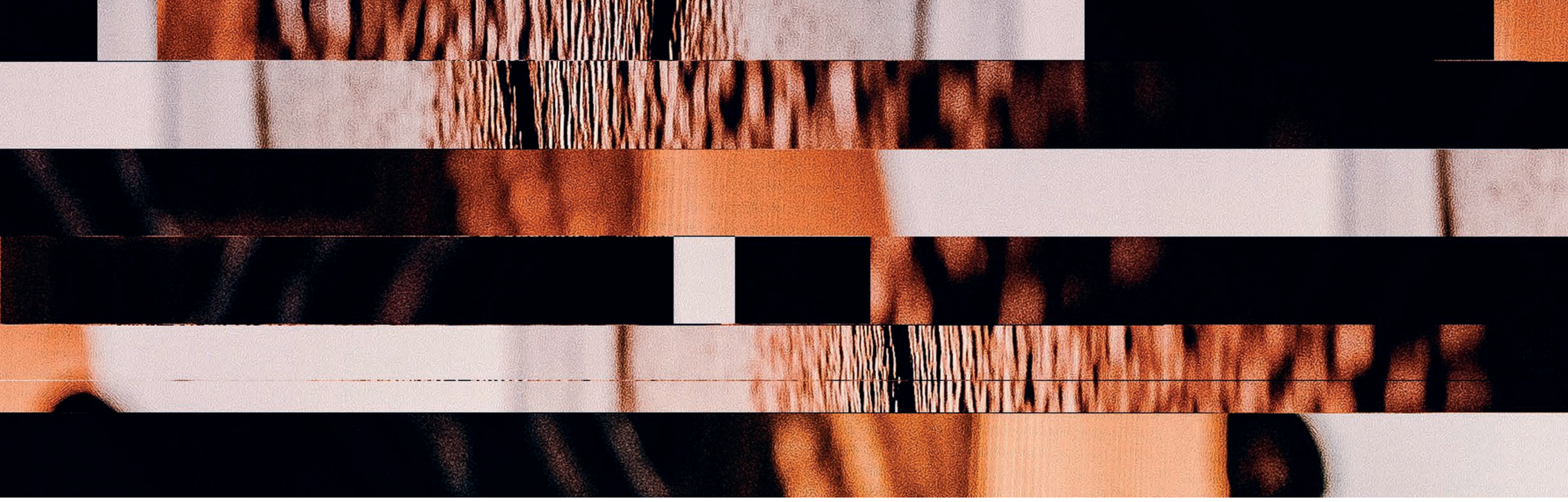
Application Fraud

Application fraud can take many forms. Using the example of an ATO again, criminals need drop accounts to receive the funds when the money is transferred out of a customer's account. While some criminals may use their own accounts, the ideal scenario is to create a new account. Third-party application fraud takes place when compromised personal identity information (PII) is used to open an account. The account can then be used for a variety of activity, including as a drop account.

Synthetic Identity Fraud

Some fraudsters are turning to a different type of application fraud that is wreaking havoc in the United States, Synthetic Identity Fraud. Synthetic Identity Fraud is when a fraudster pieces together fake identity data, or a combination of fake and real identity data, to establish a fabricated identity. The identity is established when the fraudster applies for credit for the first time and is declined because they have no credit on file. Although he or she is declined, a record of that identity is created, and the fraudster can then easily build up a credit score to a point where the application will be approved. For this attack to succeed there is a heavy reliance on a social security number, hence the reason for its prevalence in the US.

Once this is accomplished the fraudster can use the account as they please. Often, they work to build up their credit score to gain access to larger lines of credit, with the end game to bust out for financial gain. However, these accounts are also useful as drop accounts for money being fraudulently transferred out of a customer's accounts.



ARIC platform has been selected by HSBC to support efforts to strengthen Anti-Money Laundering and fraud prevention in the insurance and retail fields respectively.

HSBC

Money Laundering & Money Mules

A challenge associated with criminal activity is how to account for any illegal proceeds without raising suspicion. And the process of legitimizing these proceeds is of critical importance. It means that criminals can then begin to enjoy these profits without jeopardizing the source of income.

Currently, one of the methods most used in money laundering is through the recruitment of money mules. In this tactic unsuspecting individuals are solicited with opportunities to make quick and easy money on the side. The execution is usually nothing more than a simple set of instructions to an individual to move money from point A to point B, or by gaining direct access to the account. Criminals put tremendous effort into legitimizing the opportunity to sell people on opting in, but it is surprising how little convincing it can take.

FATF

The United Nations Office on Drugs and Crime (UNODC) conducted a study to determine the magnitude of illicit funds generated by drug trafficking and organized crimes and to investigate to what extent these funds are laundered. The report estimates that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered.

Financial Action Task Force

ARIC™ Risk Hub

> “The growth in fraud, as well as the sophisticated forms that attacks take, forces payments ecosystem participants to seek innovative and disruptive solutions to reduce fraud and make manual processes more efficient, without sacrificing customer experience.”
>
> **Juan Carlos Viramontes,**
> **MIT CEO**

Mitigating Financial Crime in Instant Payment Schemes

The criminal tactics discussed are by no means a finite list. Financial crimes take many forms and continues to evolve in line with the pace of innovations to prevent financial crime.

Featurespace’s ARIC™ Risk Hub offers a holistic solution to protect your business and customers from financial crimes. We achieve this through our invention - Adaptive Behavioral Analytics technology - which combines real-time machine learning and Adaptive Behavioral Biometrics to monitor individual customer data, detect anomalies and block new financial crimes as it occurs.

Holistic machine learning system

Financial criminals' techniques are constantly evolving, which means that traditional systems are always playing catch up: a model that begins strongly can degrade over time. ARIC Risk Hub leverages granular behavioral profiles that detect changes as they occur, resulting in truly adaptive models. Also, it's incredibly important to monitor both outbound and inbound payments, therefore ARIC ingests all payment channels to provide comprehensive protection.

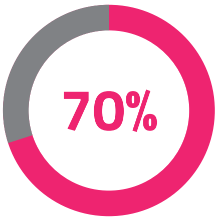
Advanced anomaly detection

ARIC's approach uses unique Adaptive Behavioral Analytics to focus on 'good' behavior to reduce false positives, reduce operational costs, and meet compliance requirements without compromising on customer experience. Furthermore, because the system is self-learning, it does not require manual retrains, and grows even more intelligent over time as the models adapt to new customer data. This results in an automated cycle of continuous improvement in detection rates.

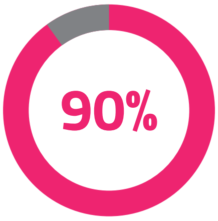
Adaptive Behavioral Biometrics

Alongside best-of-breed machine learning, ARIC's Adaptive Behavioral Biometrics uses behavioral data on websites and mobile apps to detect new fraud and specific attacks such as man-in-the-middle (MITM), Account Takeover and APP Scams, all in real time.

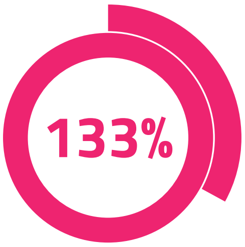
A number of features are tracked including the way a user types on a keyboard, mouse movements or tap behavior. The time spent between text fields, and system features such as device, browser, operating system and time zone are also tracked to produce a session fingerprint.



Reduction in genuine transactions declined



Fraud blocked in real-time (Credit Reference Agency)



More suspicious activity identified

One customer, a global credit card issuer, saw the number of genuine transactions declined, reduced by over 70%.

Spot more fraud and reduce false positives

Having worked with a variety of financial institutions, Featurespace helps reduce financial crime as well as friction.

Built to Scale with you

With 7 machine learning solutions from 1 Risk Hub, fraud and anti-money laundering analysts can prioritize alerts and detect suspicious activity in real time, with explainable anomaly detection, with the ARIC Risk Hub.

ARIC Risk Hub

7 Solutions to Outsmart Risk

ARIC for Card Fraud Prevention

ARIC for Payment Fraud Prevention

ARIC for Application Fraud Prevention

ARIC for Merchant Monitoring

ARIC for Anti-Money Laundering

ARIC for Gaming Fraud Prevention

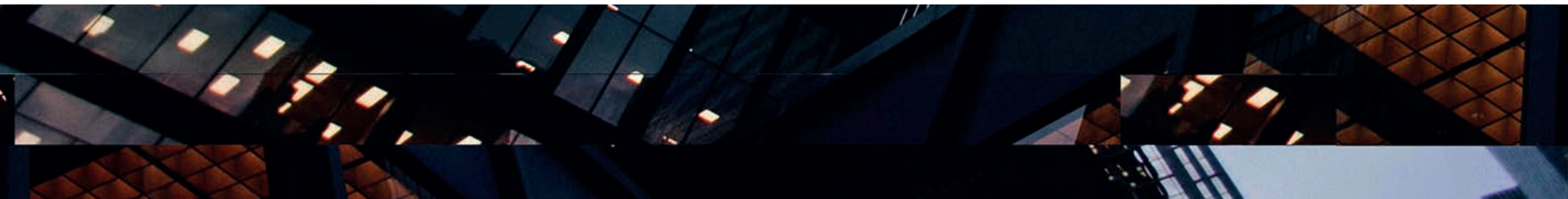
ARIC White Label

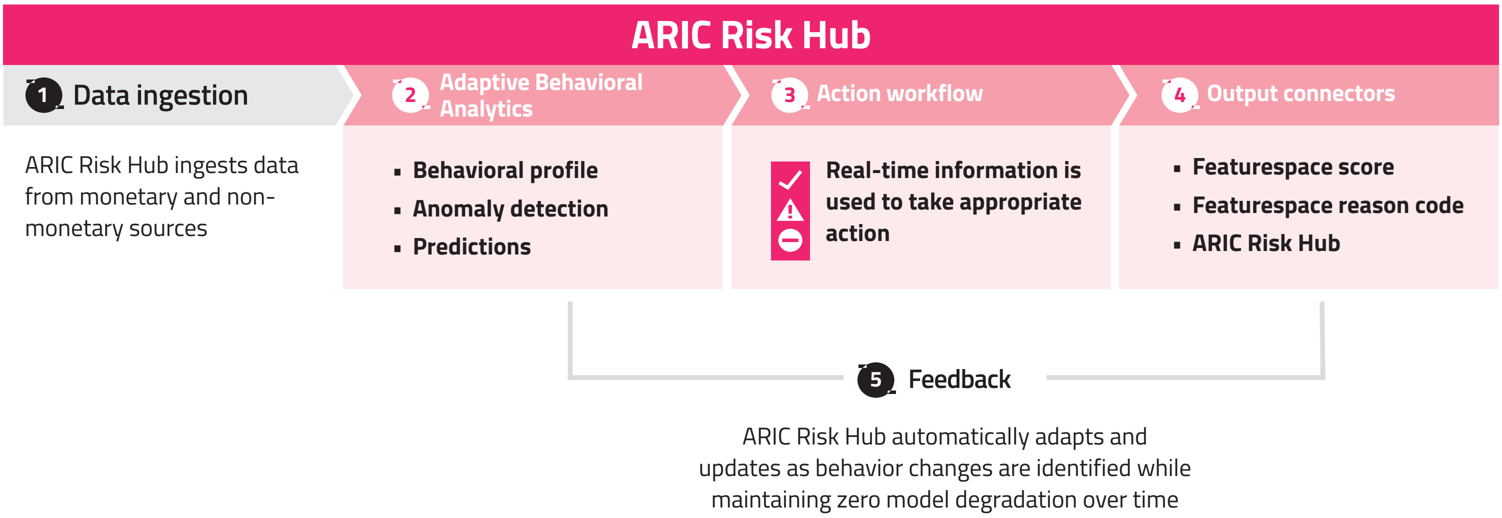
Multi-tenant capabilities across all solutions

Real-time risk management

The most important component of preventing financial crime in instant payment schemes is being able to profile and output a risk score in real-time. This may seem obvious, but not all risk engines are compatible with real-time scoring and do not process events in a manner that is needed for real-time payments.

ARIC Risk Hub builds individual profiles by analyzing good behavior, spotting suspicious activity and by using real-time transaction monitoring to catch 75% of fraud across types.





ARIC Risk Hub

1 Data ingestion

ARIC Risk Hub ingests data from monetary and non-monetary sources

2 Adaptive Behavioral Analytics

- Behavioral profile
- Anomaly detection
- Predictions

3 Action workflow

✓ ⚠ ⊖ Real-time information is used to take appropriate action

4 Output connectors

- Featurespace score
- Featurespace reason code
- ARIC Risk Hub

5 Feedback

ARIC Risk Hub automatically adapts and updates as behavior changes are identified while maintaining zero model degradation over time

Technological approach

- Profiling good behaviour rather than pattern-matching bad behaviour
- Unique real-time Adaptive Behavioural Analytics

Platform architecture

- Self-learning models do not degrade
- Reduces operational cost of updating fraud systems internally

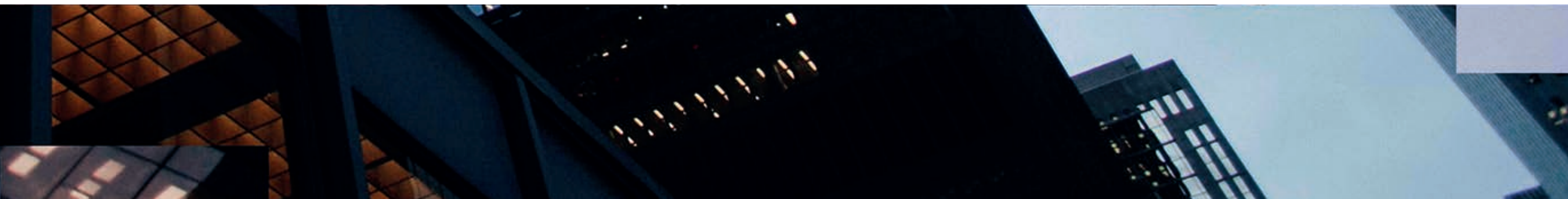
Deployment

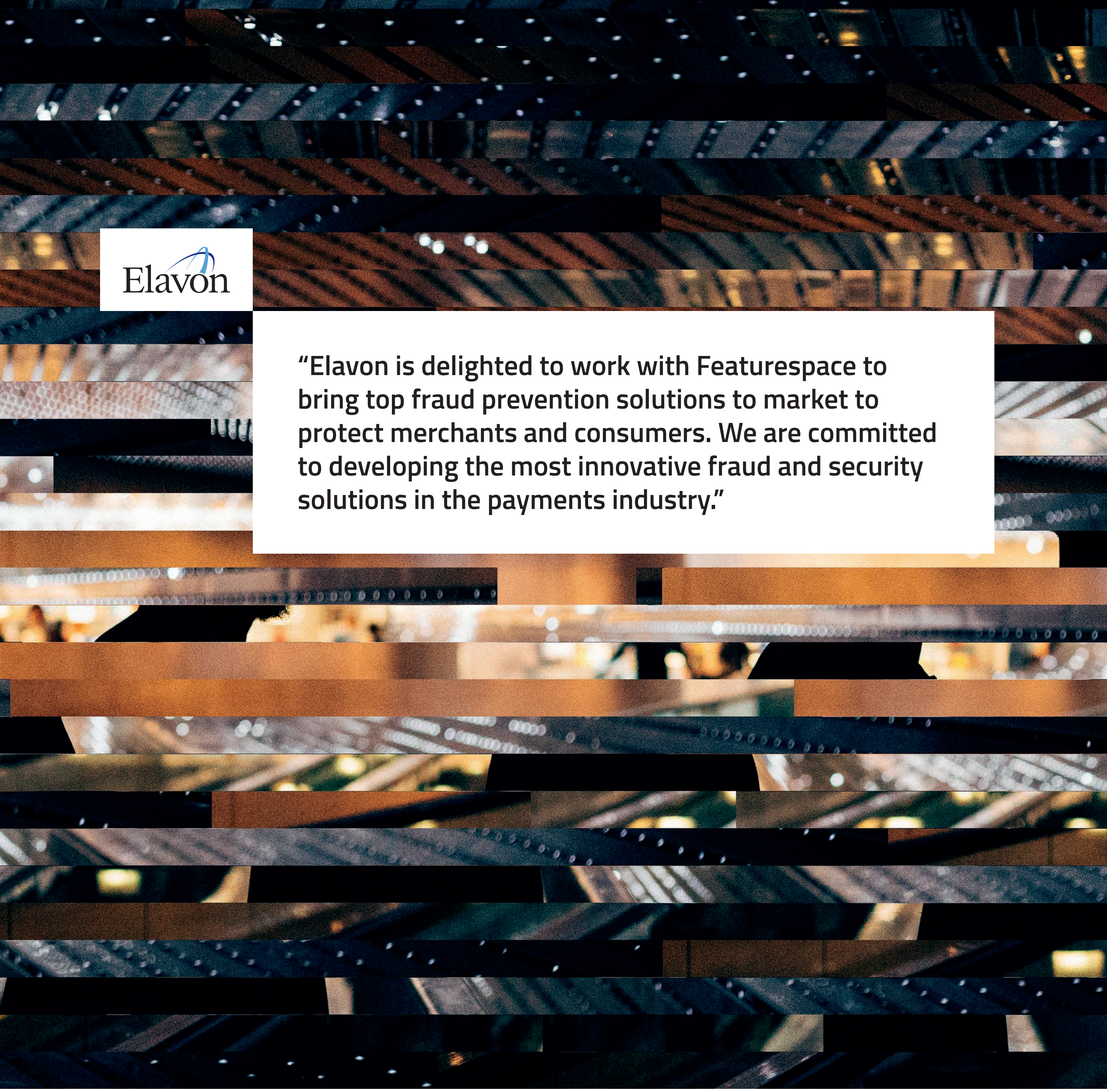
- Quick deployment
- Cloud or on premise
- Low latency
- Data management according to requirements

Conclusion

Instant payment schemes such as Real-Time Payments (US), Faster Payments (UK) and the New Payments Platform (AUS) are a reality and is evidence that future innovations in finance is certain.

To see the success of any financial crime prevention strategy, ensure that current approaches can easily scale alongside future change. Digital transformation continues to be a core part of businesses' strategic objectives. This will not change, and it is not going away. Aligning the technology used to accurately detect and prevent financial crimes in real-time is a key part of any digital transformation strategy for financial institutions.





Elavon

"Elavon is delighted to work with Featurespace to bring top fraud prevention solutions to market to protect merchants and consumers. We are committed to developing the most innovative fraud and security solutions in the payments industry."

About Featurespace

Born out of 30 years of research at Cambridge University

Trusted by the most respected banks and payments companies in the world

World leaders in machine learning for solving risk challenges

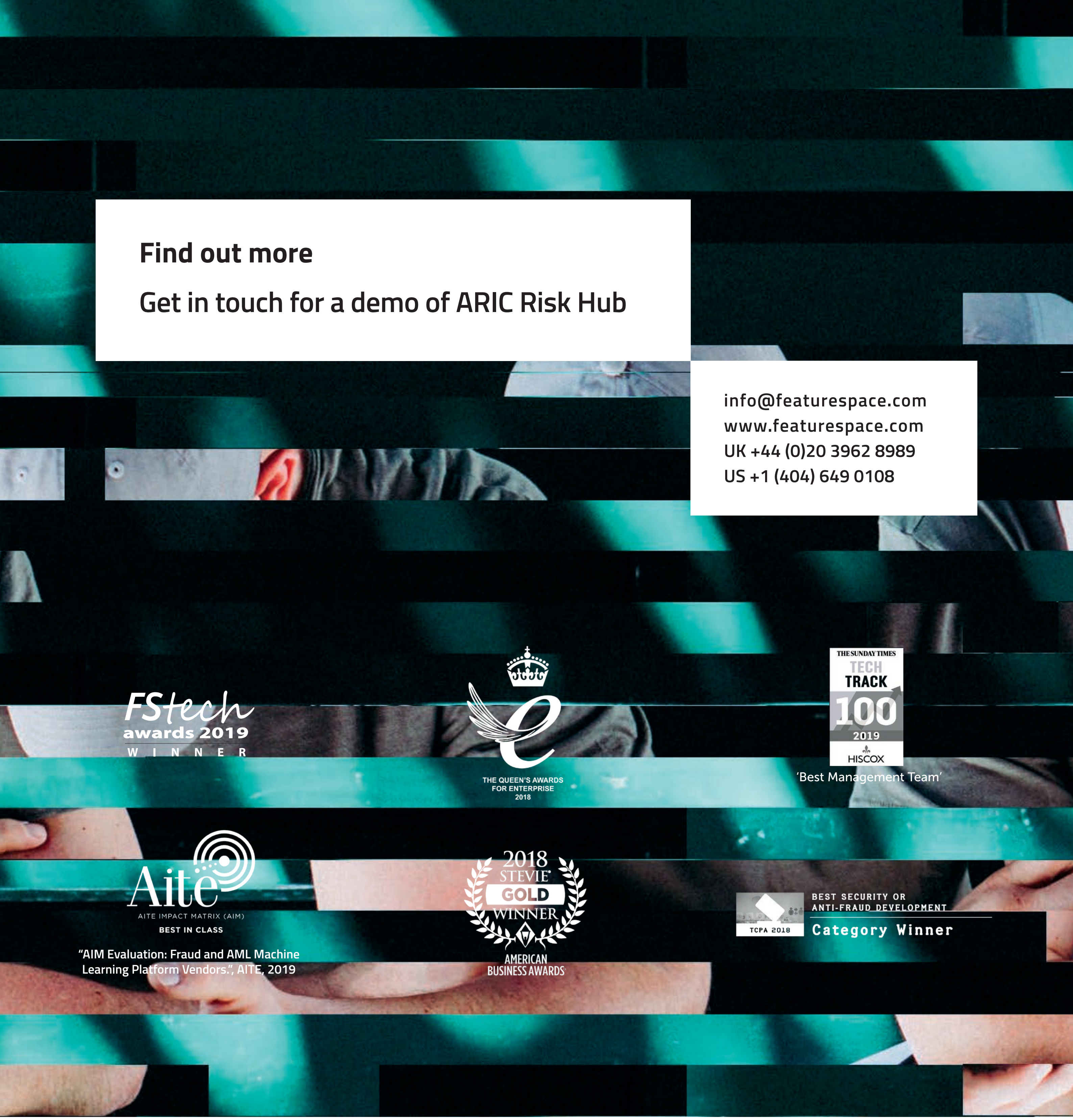
“Featurespace ARIC named “best in class” among the new generation of AML solutions in the 2019 AITE report “AIM Evaluation: Fraud and AML Machine Learning Platform Vendors.”

Aite

Unique real-time machine learning methodology

Multi-award winning platform and best machine learning models

Inventors of Adaptive Behavioral Analytics



Find out more

Get in touch for a demo of ARIC Risk Hub

info@featurespace.com
www.featurespace.com
UK +44 (0)20 3962 8989
US +1 (404) 649 0108

FStech awards 2019 WINNER

THE QUEEN'S AWARDS FOR ENTERPRISE 2018

THE SUNDAY TIMES TECH TRACK 100 2019 HISCOX

'Best Management Team'

Aite AITE IMPACT MATRIX (AIM) BEST IN CLASS

"AIM Evaluation: Fraud and AML Machine Learning Platform Vendors.", AITE, 2019

2018 STEVIE GOLD WINNER AMERICAN BUSINESS AWARDS

TCPA 2018 BEST SECURITY OR ANTI-FRAUD DEVELOPMENT Category Winner

Cambridge

Featurespace,
Broers Building,
21 JJ Thomson Avenue,
Cambridge, CB3 0FA
United Kingdom

Atlanta, GA

Featurespace,
600 Peachtree Street NE,
Suite 420
Atlanta, Georgia 30308
United States of America

London, UK

Featurespace,
15th Floor,
110 Bishopsgate,
London, EC2N 4AY
United Kingdom