Securing Payments in an ever-changing landscape

James Richardson, Head of Market Development – Risk & Fraud
Rob Scriven, Group Treasurer & Planning Manager – Cairn Energy

BUSINESS PAYMENTS BAROMETER 2017: SNAPSHOT

UK Financial decision makers surveyed

Relative Y/Y increase in the concern of Insider Payment Fraud

Businesses unaware if they have been impacted by Payment Fraud

The need for greater security

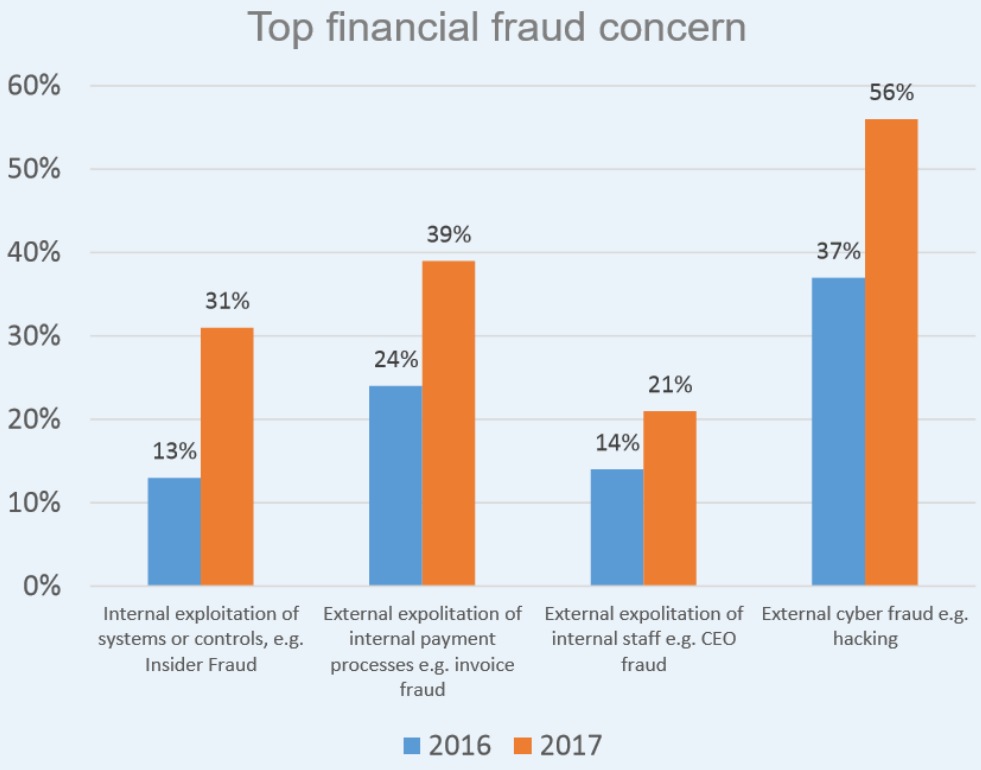
Greatest single driver of change in the payments industry in next 12 months

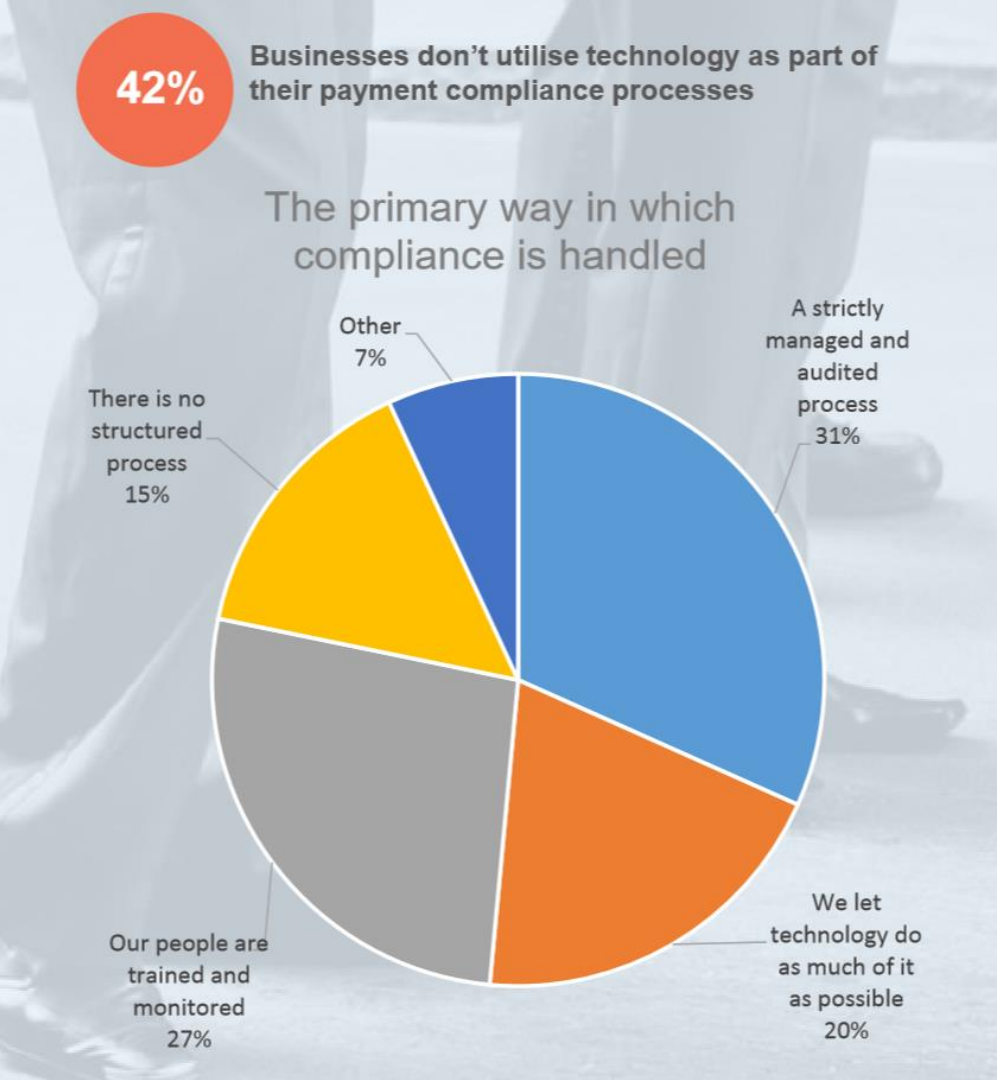
Bottomline Technologies

Internal Payment Fraud a growing concern

31%

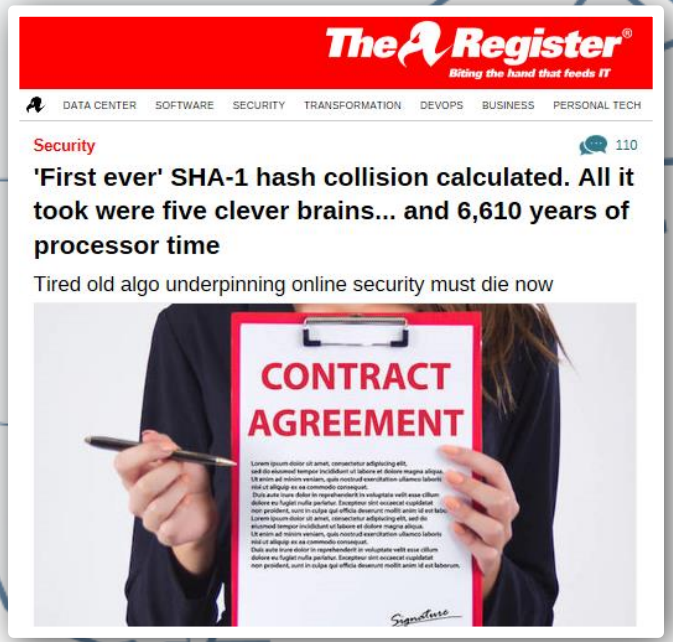
Versus 13 per cent in 2016 – a 138 per cent relative year on year increase in the concern over payment fraud committed by internal staff





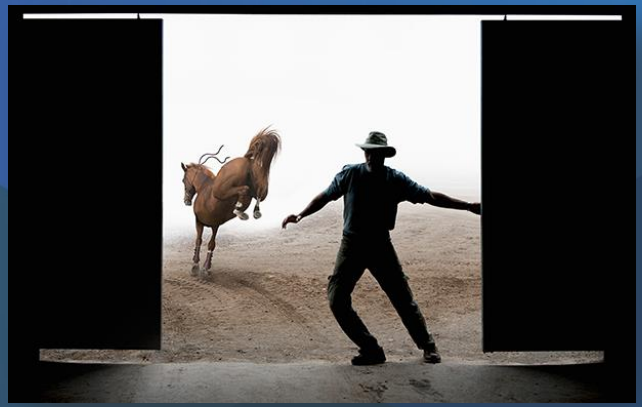
Technology needs to be integrated and ***complement*** compliance processes

6,610 years of computer processing, covered in just 10 years



Bacs TLS/SHA-2

Quick…shut that stable door!



- Spot checking
- Post submission reporting & analysis
- Transaction only monitoring

…will not totally secure your payments

Latest Cyber Frauds – Compromising Credentials

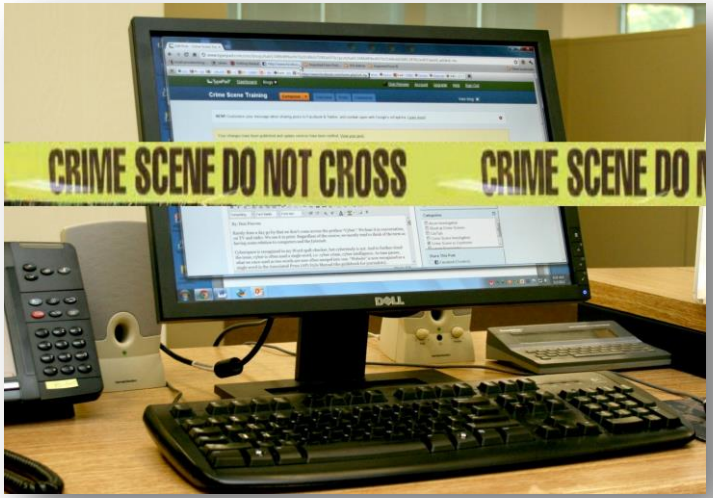
- Attackers look for valid account and password credentials from staff who have legitimate access to the payment infrastructure
- Once obtained, they are well hidden as a normal user
- Observe activity to familiarise how organisations' back office process and systems work

Latest Cyber Frauds – Fraudulent Payments

- Cyber Fraudsters log in, impersonate the operators and submit fraudulent payments
- New Users get created and removed during the payment process

Description	Value
Currency	USD & EUR
Value	$350,000 - $4,000,000, majority below $1,000,000
Time	After business hours
Country of beneficiary accounts	Switzerland, UK, Kenya, Portugal

Latest Cyber Frauds – Hide the evidence!



- Hide the evidence to extend detection period and decrease probability of cancellation
- Make the business reconciliation process more difficult
- Database alteration. Fraudulent payments and legitimate confirmations highlighting fraudulent payments get removed

SWIFT's Customer Security Programme – a sign of change?

Purpose

In response to cyber-related payment frauds, SWIFT have issued a set of core security standards and an assurance framework that will be mandatory for all SWIFT members

What does it cover?

16 mandatory and 11 advisory controls spanning 3 objectives:

- **Secure Your Environment**
- **Know and Limit Access**
- **Detect & Respond**

Urgency

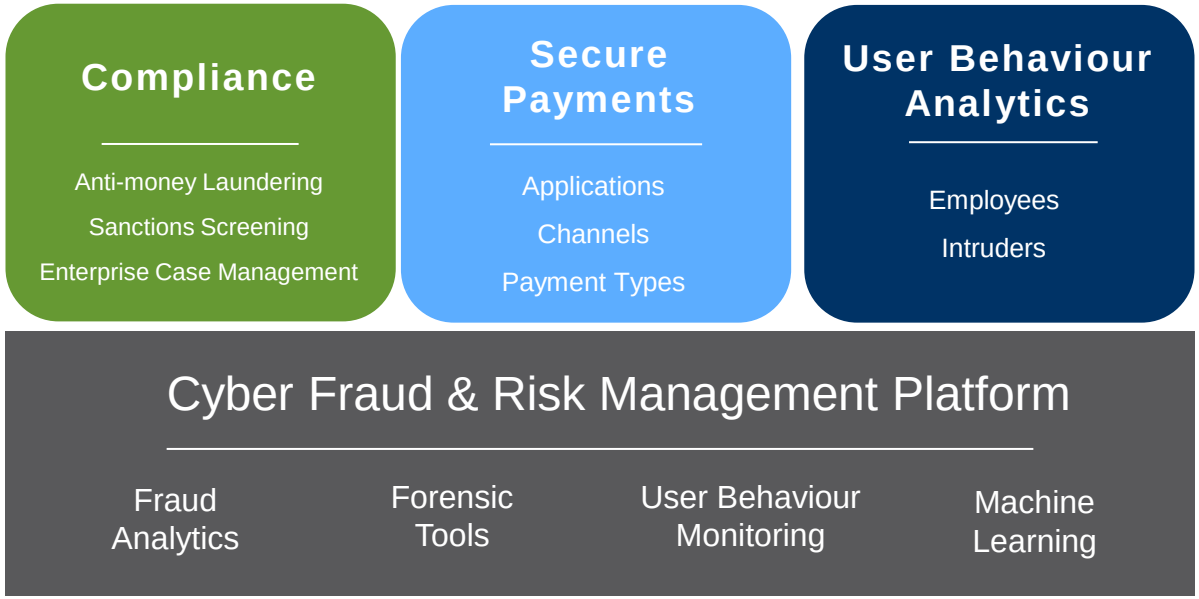
- By 31 Dec 2017 and 2018 members must declare the compliance status and be compliant with the programme

What does it mean?

- SWIFT members are responsible for reviewing their infrastructure, meeting mandatory control standards, and self-attesting by end of 2017
- SWIFT reserve the right to report non-attestation from 2018, and non-compliance from 2019
- Compliance status of individual controls visible to counterparties who are granted access

Bottomline Technologies

Technology offerings being adopted by organisations



Bottomline Technologies

Summary & Panel Discussion

- The Payment Landscape is evolving fast – are you ready?
- New compliance standards will be observed to ‘play on the pitch’
- Don’t rely on old processes to detect new Cyber Frauds