Commercial in Confidence

Grant Thornton

The next phase of fraud prevention

Data, networks and earlier intervention

25 November 2026

Agenda

1	Why prevention needs to move earlier	5
2	Earlier intervention	7
3	Data and network detection	11
4	AI-enabled fraud	16
5	Threat-led controls	20
6	Priorities for 2027 and discussion	24

Industry experts speaking today



Tom Townson
Partner
Grant Thornton UK



Alison R Kopra
Director
Grant Thornton UK

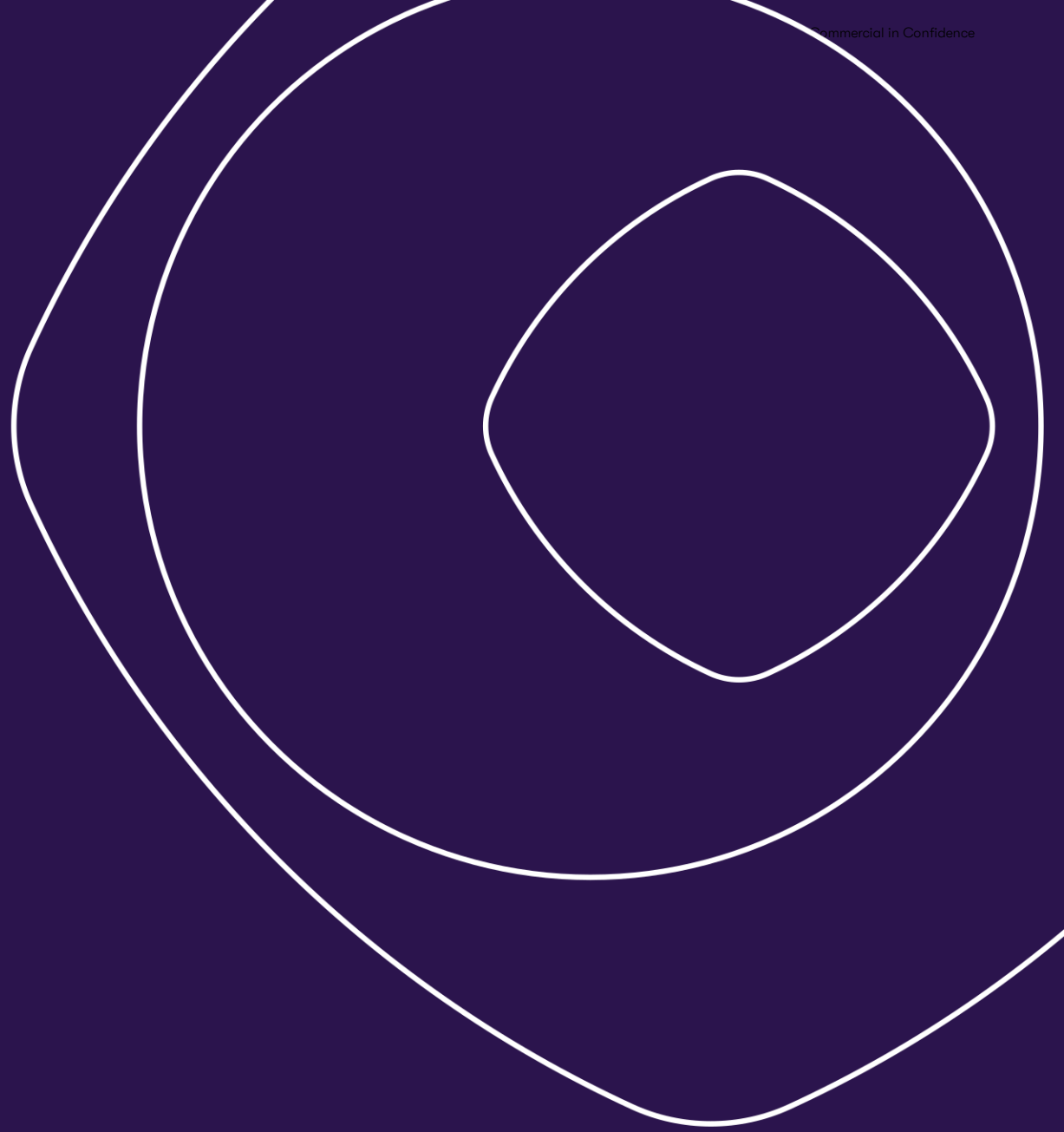


Michael FJ Carré
Associate Director
Grant Thornton UK

© 2026 Grant Thornton UK Advisory & Tax LLP.

1

Why prevention needs to move earlier



© 2026 Grant Thornton UK Advisory & Tax LLP.

By the time a payment is made, the fraud may already be well underway

66%
of APP fraud cases begin online

17%
begin through telecoms

£576 million
APP fraud losses in 2025

£153 million
in crypto-routed scams, up from £59 million

How a typical investment scam unfolds

Fake online advert
First contact, often outside the bank's view

Weeks of messages and calls
The fraudster builds credibility

A convincing platform and "returns"
Documents and dashboards look legitimate

Payment instruction
Often the first point the bank sees anything

The question is no longer only who reimburses the loss, but who could have prevented it.

UK Finance, Annual Fraud Report 2026 (2025 APP fraud data)

© 2026 Grant Thornton UK Advisory & Tax LLP.

2

Earlier intervention

Where in the journey can firms interrupt a scam, and when is intervention justified?

© 2026 Grant Thornton UK Advisory & Tax LLP.

There are multiple opportunities to interrupt a scam before money moves

Before contact	During the session	At payment	Receiving side
			
Block fraudulent messages, adverts and accounts.	Identify behavioural anomalies and signs of manipulation.	Apply targeted warnings, challenges and payment controls.	Detect mule activity and disrupt onward movement.
Telecoms and platform intelligence	**Device and behavioural signals**	**Beneficiary and payment risk**	**Account and network monitoring**

© 2026 Grant Thornton UK Advisory & Tax LLP.

Effective prevention means balancing intervention, customer friction and risk



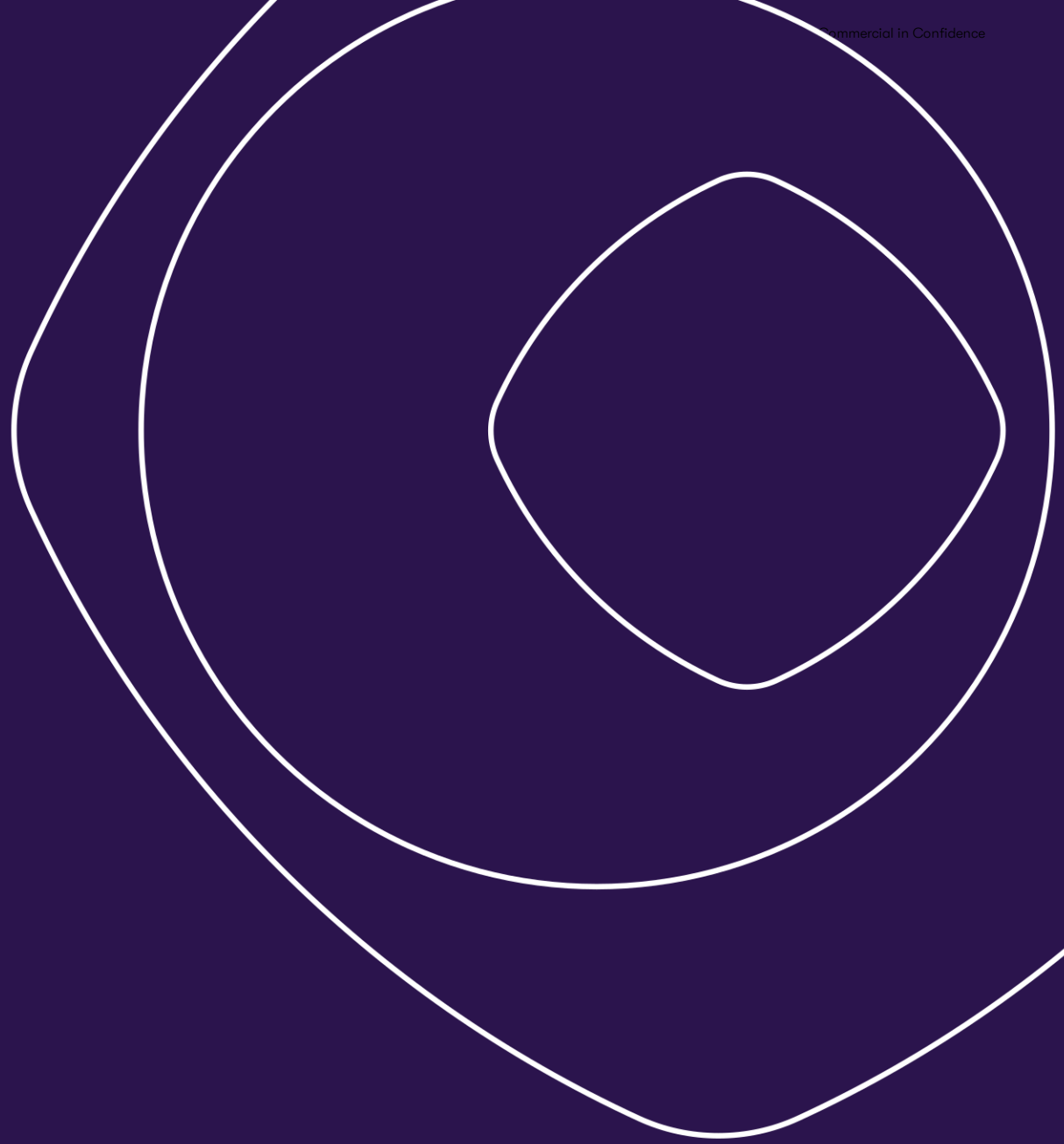
The aim is not to challenge more payments indiscriminately. It is to identify higher-risk situations accurately and apply an intervention proportionate to the risk, which should link to your firm's fraud risk assessment and defined risk appetite.

© 2026 Grant Thornton UK Advisory & Tax LLP.

3

Data and network detection

Firms already hold information that could prevent more fraud. The question is whether they connect it in time.



© 2026 Grant Thornton UK Advisory & Tax LLP.

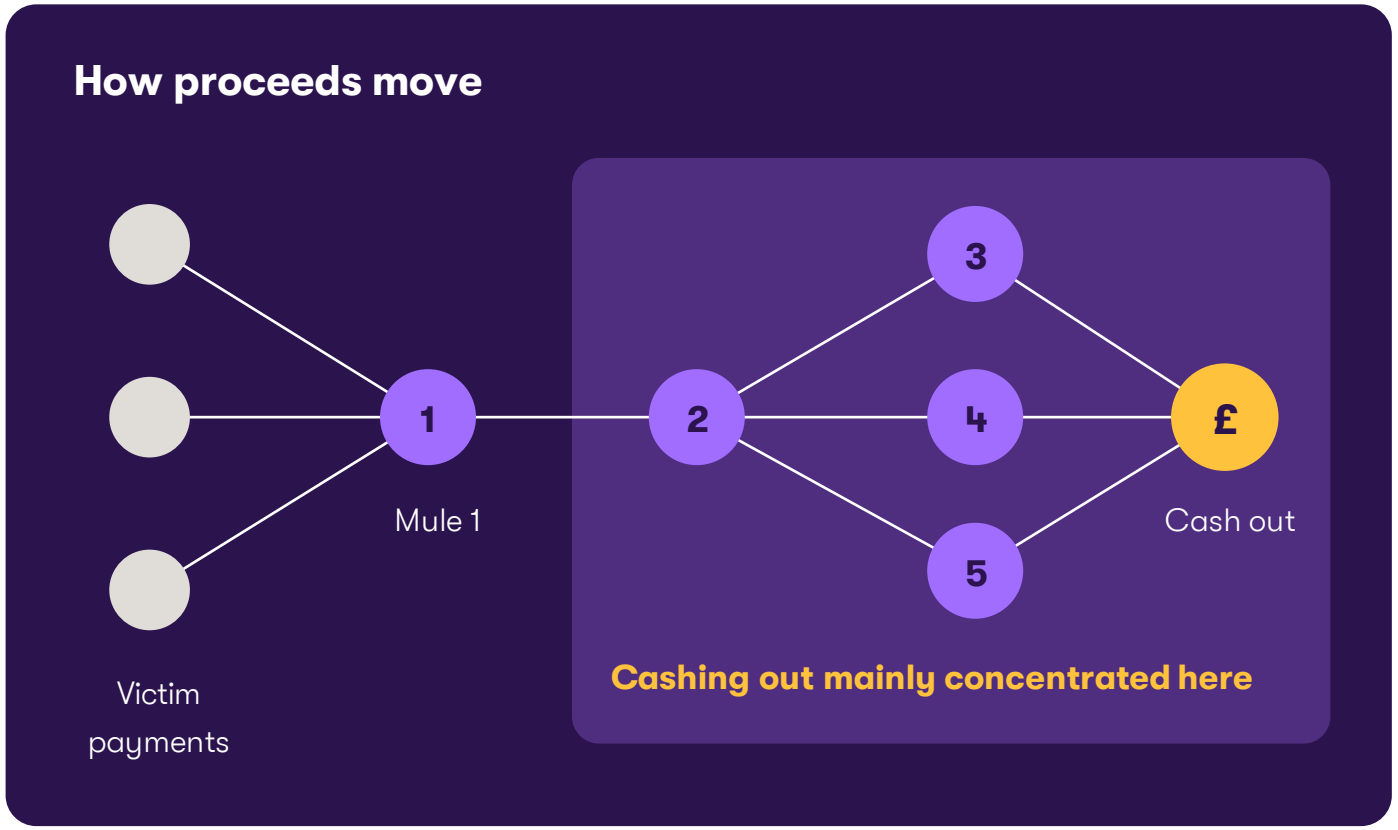
Fraud operates through networks, but firms often detect individual events

238,396

suspected mule accounts closed by surveyed firms in 2025

Between 2 and 5

Where the FCA found cashing out was mainly concentrated in the chain of mule accounts



© 2026 Grant Thornton UK Advisory & Tax LLP.

Connecting the data can reveal what individual alerts miss

Viewed individually

Account A
Incoming at 09:04
£2,200

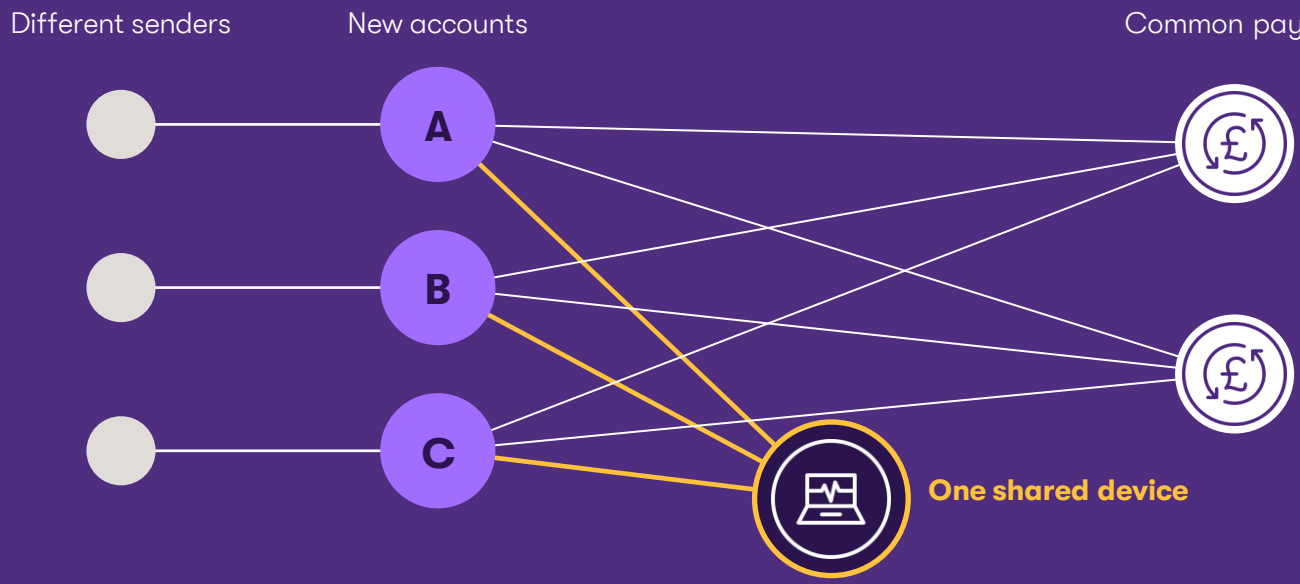
Account B
Incoming at 09:11
£2,700

Account C
Incoming at 09:18
£3,100

Separate activity, each assessed against its own customer profile

Viewed as a network

Shared device, recently opened accounts and rapid onward transfers



Customer
Account age

Device
Shared access

Beneficiary
Common payees

Transaction
Velocity

© 2026 Grant Thornton UK Advisory & Tax LLP.

Better intelligence sharing can extend chances for detection

Each step widens the view of the network, yet adds legal and operational friction



Within the firm

Connect customer, device, beneficiary and transaction data across fraud, AML and onboarding. Agree which data each function needs from the other.

Routes: Existing systems and case data

Limit: Data held in separate systems



Across financial institutions

Warn firms about customers you have acted on, and answer their requests.

Routes: ECCTA s188 and s189, Cifas, Pay.UK EDEx (in development)

Limit: Voluntary, and use is not measured publicly



Across the fraud chain, sectors

Link payment intelligence with telecoms, platform and law enforcement data.

Routes: Online Crime Centre (launched April 2026), JMLIT+, Stop Scams UK

Limit: ECCTA protections cover the regulated sector only, not platforms or telecoms



Across borders

Follow funds and networks that leave the UK, including within a global group.

Routes: Group-wide policies and law enforcement channels

Limit: ECCTA protections apply only to sharing within the UK

The Home Office describes economic crime information sharing as “technically possible” but “practically constrained” by “legal, operational and cultural barriers”. Individual firms are reluctant to risk breaching other requirements

© 2026 Grant Thornton UK Advisory & Tax LLP.

4

AI-enabled fraud

Authenticating the right customer is not the same as knowing the payment is legitimate.

© 2026 Grant Thornton UK Advisory & Tax LLP.

AI is making familiar frauds faster, cheaper and more convincing



Voice and video impersonation

Convincing impersonation of trusted people in calls or video.



Document forgery, synthetic identities

Synthetic identity documents, statements and supporting evidence. An increasing risk for insurers especially.

77%

of surveyed anti-fraud professionals reported increased deepfake social engineering over the preceding two years

ACFE/SAS global survey, March 2026



Scams at scale

Personalised messages, investment scams, sustained manipulation, and grooming the fraudsters of the future.



Digital injection attacks

Deepfake media injected into remote identity verification.

A valid payment may not be a legitimate payment. The speed, credibility and scale of fraud is changing, with AI lowering the barriers to entry, and increasing overlap with county lines criminality.

© 2026 Grant Thornton UK Advisory & Tax LLP.

Technology can strengthen the defence, but controls need to evolve



Is this the genuine customer?

Threats

Deepfakes, synthetic identities, account compromise, agentic payments

Defensive controls

Physical biometrics, injection-resistant identity checks, device binding, passkeys and independent verification



Is the genuine customer being defrauded?

Threats

AI-enabled manipulation, investment scams, payment redirection

Defensive controls

Behavioural analytics, beneficiary intelligence, network detection and targeted intervention



Where AI can help

Detect unusual patterns and behaviours

Prioritise investigations and assist SAR filing

Adapt to emerging threats, with more dynamic controls

Good fraud decisions depend on the right signals, not simply more sophisticated technology.

With increasing technology adoption, getting different tools to work together to prevent fraud is both an opportunity and a practical constraint.

© 2026 Grant Thornton UK Advisory & Tax LLP.

5

Threat-led controls

How quickly can firms turn what they learn about fraud into controls that work?

© 2026 Grant Thornton UK Advisory & Tax LLP.

Fraudsters adapt faster than traditional control-change processes

Control introduced	Criminal adaptation
Stronger authentication Two-factor authentication	**Passcode manipulation and SIM swapping**
Improved message filtering Blocking fraudulent SMS	**New formats and messaging channels**
Transaction monitoring Value and velocity thresholds	**Payment splitting and multi-account movement**

Control effectiveness changes as criminal behaviour changes.

© 2026 Grant Thornton UK Advisory & Tax LLP.

Firms need a repeatable process for turning intelligence into action



Identify Recognise the emerging pattern across cases and intelligence

Assess Understand the exposure and why existing controls missed it

Prioritise Decide what intervention is justified, and who owns it

Change Implement and test the response before scaling it

Measure Establish whether the control actually reduced fraud

Technology can shorten the cycle

- Connected intelligence
- Faster analysis and triage
- Controlled rule changes

© 2026 Grant Thornton UK Advisory & Tax LLP.

The real measure is whether controls prevent fraud

Measure	What it tracks	What it tests
Prevention	Fraud losses and estimated losses prevented	**Impact**
Detection	Confirmed fraud identified before funds move	**Timeliness**
Accuracy	Genuine fraud versus unnecessary interventions	**Precision**
Customer outcomes	Legitimate payments delayed or declined	**Friction**
Adaptability	Time from emerging threat to effective control change	**Responsiveness**

More alerts do not necessarily mean better fraud prevention – and controls need consistent challenge and an effective culture within your organisation.

© 2026 Grant Thornton UK Advisory & Tax LLP.

Three priorities for fraud prevention over the next 6 to 12 months

1



Intervene earlier

Map the fraud journey and test where existing interventions succeed or fail.

Output
Intervention gaps and improvement priorities

2



Connect data and intelligence

Find ways to detect relationships across customers, devices, beneficiaries and transactions, and ensure teams understand how to use these tools.

Output
Prioritised data and detection improvements, feedback loops

3



Adapt and measure

Cut the time from emerging intelligence to control change through effective governance and response

Output
Owned change process and effectiveness measures

© 2026 Grant Thornton UK Advisory & Tax LLP.

Questions



© 2025 Grant Thornton UK Advisory & Tax LLP.

Get in touch



Tom Townson
Partner
Grant Thornton UK
T:+44(0)207 865 2175
E:Thomas.F.Townson@uk.gt.com



Alison R Kopra
Director
Grant Thornton UK
T:+44(0)207 865 28177
E:Alison.R.Kopra@uk.gt.com



Michael FJ Carré
Associate Director
Grant Thornton UK
T:+44(0)207 865 2880
E:Michael.FJ.Carre@uk.gt.com



© 2026 Grant Thornton UK Advisory & Tax LLP.



© 2026 Grant Thornton UK Advisory & Tax LLP. All rights reserved. 'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton UK Advisory & Tax LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.