Anti-Fraud and Anti-Theft Policy

I. Introduction and Purpose

At CRH, our values unite us in the way we work, all over the world. They are the foundation of our culture, as set out in our Code of Business Conduct.

This Anti-Fraud and Theft Policy (the “Policy”) aids in the prevention, detection, and investigation of fraud and theft, safeguarding CRH’s assets and providing protection from the legal and reputational consequences of fraudulent activities.

CRH has identified Fraud Points of Contact (“POCs”) within the businesses, who are a local resource for inquires related to fraud and theft and are responsible for reporting suspected, attempted, and actual frauds and thefts for their businesses. (See Fraud Point of Contact List). The Fraud POCs will work with Risk & Internal Controls, Internal Audit, Legal & Compliance, Treasury, Security, and Information Security in the execution of this Policy.

II. Statement of Policy

CRH does not tolerate fraud or theft and requires that CRH employees and third parties acting on CRH’s behalf work with honesty and integrity consistent with the Code of Business Conduct. CRH requires each employee and third party to be vigilant about the risk of fraud or theft and ensure that CRH does not become a victim of such conduct.

Each CRH employee has a duty to report any actual, suspected, or attempted fraud or theft as set out in Section III below.

Fraud is intentionally making a false representation or failing to disclose information for personal gain and/or to cause loss to another. Theft is taking of another’s property without their consent. Both fraud and theft can be criminal. Examples of fraud and theft include but are not limited to:

- stealing cash/product from a CRH company
- falsification of records
- an external party stealing CRH equipment
- misuse of company assets for personal gain
- misrepresenting personal expenses as business expenses disciplinary action.
- misrepresenting a product that is sold to a customer
- a cyber-attack that results in a fraudster gaining access to CRH’s IT systems, employees’ identities, online accounts, or bank accounts (“Cyber Fraud”) and
- a falsified payment instruction to withdraw funds from a CRH bank account (“Payment Fraud”) (when this occurs as a result of collecting information by accessing CRH or its employees’ email or data systems, it is both Cyber Fraud and Payment Fraud).

Failure to comply with this Policy, including failure to report instances of fraud or theft, may lead to disciplinary or legal action.

Non-Retaliation

CRH does not tolerate retaliation for reporting a genuine concern.The business will investigate any suspected retaliation and take appropriate action, including disciplinary action. If at any time an employee feels they have been retaliated against for reporting a concern of fraud or theft, they should contact their local Legal and Compliance contact or www.crhhotline.com.

III. Roles and Responsibilities

Employees must:

- Read the Code of Business Conduct and understand the behaviour expected of them
- Read and understand the requirements of this Policy
- Use CRH and third-party assets, resources, and funds honestly
- Report actual, suspected, or attempted fraud/theft immediately (within 24 hours) in one of the following ways (See Fraud and Theft Reporting Decision Tree in Appendix 1):
  - To a line manager or any member of the business’s management team
  - To your local Fraud Point of Contact (Fraud POC) (See Fraud Point of Contact List)
  - To the confidential CRH Hotline: www.crhhotline.com
  - If a Payment Fraud: email paymentfraud@crh.com and notify the relevant Fraud POC (if the Payment Fraud took place via Cyber Fraud, also notify CRH’s Information Security Team at cyber@crh.com) and liaise with Group Treasury and the relevant bank to freeze, recover or secure any funds at risk.
- Participate in any relevant training programme provided

Business management must*:

- Inform employees of who their Fraud POC is and that all frauds and thefts should be reported promptly to the Fraud POC*
- Lead and embed an anti-fraud/anti-theft culture in the business
- Ensure that employees participate in any relevant training programme provided
- Ensure reported frauds/thefts are investigated by an independent person and appropriate action is taken
- Establish and operate adequate controls and procedures to prevent and detect fraud/theft, including deterring fraud/theft
- Review fraud/theft risk assessment and mitigation activities regularly
- Complete an annual fraud/theft risk assessment

Fraud POCs and Internal Controls must*:

- Work together with business management to inform employees of who their Fraud POC is and that all frauds and thefts should be reported immediately to the Fraud POC*
- Report and escalate frauds/thefts as provided in this Policy and the Anti-Fraud and Theft Reporting Procedures
- Along with business management, ensure reported frauds/thefts are investigated by an independent person and appropriate action is taken

* Additional resources are available to assist with these responsibilities (See Section V for contact information).

Anti-Fraud and Anti-Theft Policy continued

IV. Monitoring, Assurance and Breach Reporting

Monitoring and Assurance

Each business is responsible for the operation and monitoring of fraud and theft prevention and detection control measures in the business. Internal Audit reviews the effectiveness of controls through audit risk assessments, SOX testing, and assessment of internal controls. Legal and Compliance provides legal advice, fraud risk assessment, fraud investigation, recovery actions, and training programmes. Additionally, fraud and theft risk is assessed regularly as part of CRH's risk management processes.

Investigations and Outcomes

CRH will investigate all actual, suspected, or attempted fraud or theft and seek to recover any losses sustained. Each business will follow disciplinary procedures, up to and including dismissal, in accordance with local law. CRH may report criminal conduct to local law enforcement agencies in accordance with local law.

V. Relevant Contact Details

In the event of any questions regarding this Policy or concerns of fraud or theft, please contact your local Legal and Compliance contact or any of those listed below. Additionally, any good faith concerns of fraud or theft can be reported to the CRH Hotline, which allows for anonymous reporting: www.crhhotline.com.

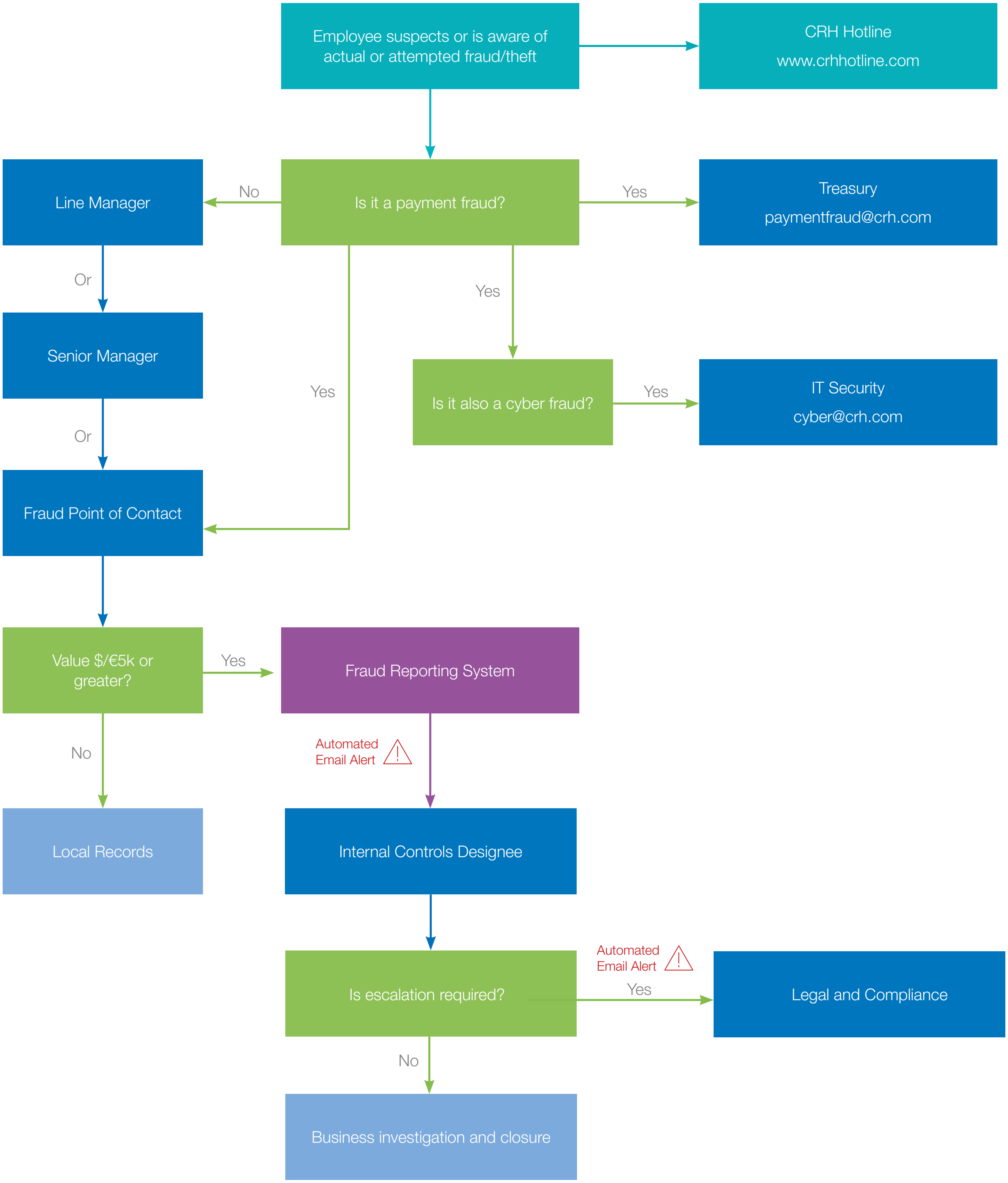
Responsibility	Name	Email	Direct Dial
Legal & Compliance			
Global Head of Compliance	Elizabeth Upton	eupton@crh.com	+353 87 256 1045
Europe/Asia – Compliance Manager	Barbara Przedpelska	bprzedpelska@crh.com	+48 600 806 505
North America – Compliance Manager	Martha Burke	martha.burke@crh.com	+1 770 392 5306
Europe/Asia – General Counsel	Niamh Flood	nflood@crh.com	+353 87 622 0451
North America – Vice President & General Counsel	Dave Toolan	david.toolan@crh.com	+1 404 216 8706
Internal Audit			
Head of Internal Audit	Alan Nash	anash@crh.com	+353 87 231 7911
North America - VP Internal Audit	Misty Silverwise	misty.silverwise@crh.com	+1 770 804 3363
Europe/Asia & IPG - Director of Internal Audit	Conor Cronin	ccronin@crh.com	+353 86 008 0765
Treasury			
Group Treasurer	Anthony Fitzgerald	afitzgerald@crh.com	+353 86 385 3490
Cyber Security			
Chief Information Security Officer	Paul Clarges	pclarges@crh.com	+353 1 404 1000
Security			
Global Head of Security	Cindy Coppola	cindy.coppola@crh.com	+1 714 309 2797
Europe/Asia – Director of Security	Gilad Wax	gwax@crh.com	+34 650 089 718
Internal Controls			
North America	Danielle Hampton	danielle.hampton@crh.com	+1 678 205 9364
Europe/Asia	Darragh Sheehan	dasheehan@crh.com	+353 86 394 5176

VI. Supplementary Documentation

- Anti-Fraud and Theft Reporting Procedures
- Fraud Point of Contact List
- Code of Business Conduct

Appendix 1

Fraud and Theft Reporting Decision Tree


Employee suspects or is aware of actual or attempted fraud/theft
CRH Hotline
www.crhhotline.com
Is it a payment fraud?
No
Line Manager
Yes
Treasury
paymentfraud@crh.com
Or
Senior Manager
Yes
Yes
Is it also a cyber fraud?
Yes
IT Security
cyber@crh.com
Or
Fraud Point of Contact
Value $/€5k or greater?
Yes
Fraud Reporting System
Automated Email Alert
No
Local Records
Internal Controls Designee
Automated Email Alert
Yes
Is escalation required?
Legal and Compliance
No
Business investigation and closure