Quentin & Dundee

Fraud & Impersonation Awareness

How to verify a Q&D communication and report suspicious use of our name.

Effective September 26, 2026

PUBLIC

1. Verify before you act

Fraudulent messages, websites, and social profiles can misuse an organization’s name or visual identity. A familiar logo, display name, or apparent email address is not enough to establish who sent a message.

Our public website is quentindundee.com. If a message claims to come from Quentin & Dundee and you are uncertain, start a new conversation using the contact details published on this website or a contact you have independently verified. Do not use the links, telephone numbers, or reply instructions in the suspicious message to verify it.

2. Warning signs

Pause when a communication creates unusual urgency, demands secrecy, or asks you to bypass your organization’s normal controls. Be particularly cautious about:

- Unexpected changes to invoices, bank details, payment recipients, or instructions for transferring money.
- Requests for passwords, verification codes, identity documents, donor lists, or sensitive institutional files through an unverified channel.
- Recruiting messages that request application fees, equipment payments, gift cards, cryptocurrency, or the movement of money through your personal account.
- Unsolicited offers claiming that Q&D can guarantee a grant, donation, contract, investment return, or campaign outcome.
- Lookalike domains, shortened links, unexpected attachments, or requests to install software or give remote access.

3. Payments and sensitive information

Confirm payment arrangements against your signed agreement and independently verify any change with an established contact. The public Q&D website does not accept donations, process engagement payments, or collect account passwords.

Agree on an appropriate method with your Q&D contact before sharing confidential records. Do not send passwords or one-time verification codes. For recruiting questions, use careers@quentindundee.com to verify the opportunity before providing sensitive information.

4. Report a concern

Report suspected impersonation, fraudulent communications, or a website security concern to security@quentindundee.com. Include the claimed sender, relevant domain or page, date, and a brief description. Screenshots or message headers can help; do not forward active malware, passwords, or unnecessary personal information.

If you have sent money, contact your bank or payment provider promptly. If an account may be compromised, use the provider's official recovery channel and notify your organization's security team. Preserve the relevant messages and consider reporting the incident to the appropriate authorities. Reporting a concern to Q&D does not replace those steps or guarantee recovery.

Quentin & Dundee

QUENTINDUNDEE.COM