How to Protect Your Business
from Business Email Compromise (BEC) Scams

Companies of all sizes are being targeted by criminals through Business Email Compromise (BEC) scams. In these scams, cybercriminals gain access to an employee's legitimate business email through social engineering or computer intrusion. The criminal then impersonates the employee — often a senior executive or someone who can authorize payments — and instructs others to transfer funds on their behalf. According to the FBI, more than $3 billion has been loss due to these scams. This is a difficult scam to detect because the hackers are using legitimate email accounts to authorize wire transfers. Companies can protect themselves and their employees through education and layered authorization procedures.

Windsor Federal Savings recommends the following tips to help businesses and employees avoid Business Email Compromise scams:

- **Educate your employees.** You and your employees are the first line of defense against business email compromise. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

- **Protect your online environment.** It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

- **Use alternative communication channels to verify significant requests**. Have multiple methods outside of email – such as phone numbers, alternate email addresses – established in advance through which you can contact the person making the request to ensure it is valid.

- **Be wary of sudden changes in business practices or contacts**. If an employee, customer or vendor suddenly asks to be contacted via their personal e-mail address, verify the request through known, official and previously used correspondence as the request could be fraudulent.

- **Be wary of requests marked "urgent" or "confidential.** Fraudsters will often instill a sense of urgency, fear or secrecy to compel the employee to facilitate the request without consulting others. Use an alternative communication channel outside of email to confirm the request.

- **Partner with your bank to prevent unauthorized transactions.** Talk to your banker about programs that safeguard you from unauthorized transactions such as call backs, device authentication and multi-person approval processes.

  For more tips, see the Federal Bureau of Investigation's Internet Crime Complaint Center's public service announcement.

If you fall victim to a business email compromise scam:

- Contact Windsor Federal Savings immediately at 860-688-8511 to notify them about the fraudulent transfer and request that they contact the institution where the fraudulent transfer was sent.

- Contact your local Federal Bureau of Investigation office as they might be able to freeze or return the funds, if notified quickly.

- File a complaint, regardless of dollar loss, at www.IC3.gov.