Video Transcript: Regions Vendor Payment Fraud Video

Note:
Cyber fraud music plays.

On screen: Regions Logo appears in green and fades in a circular motion, turning into a play button icon. A cursor clicks on play button.

[Voice-over] Cybersecurity should be a top concern for companies large and small.

On screen: Dark blue background fades in with a lock icon in center and animated circles surrounding it. The lock and circles continue to scale up in size while the lock fades out and animated buildings in the center of the circles. Text below: Cybersecurity should be a top concern for companies large and small.

[Voice-over] A single cyber-attack can result in major financial loss and permanent damage to your brand.

On screen: Animated solid and dotted lines enter screen from left and right towards the buildings. The circle in the center fills to a solid blue and a negative percentage number animates above the buildings while a solid gray line with an arrow below and dollar sign. Text below: Financial loss and damage to your brand

[Voice-over] One emerging way cyber criminals attack is by sneaking into your company's email network

On screen: An envelope animates in the center circle while a hook slides down and grabs the email as it sways it back and forth. Text below: Sneaking into your company's email network

[Voice-over] to trick you into sending money.

On screen: The hook throws the envelope out of the circle and morphs into a dollar icon. The dollar icon goes down into a laptop that enters the screen. Several other dollar icons follow suit. Text below: Trick you into sending money

[Voice-over] The fraudster gains access to a trusted vendor's email account or creates a fake account that is very similar.

On screen: The laptop screen morphs into an email login screen with fraudster icon above. A cursor enters the screen and selects the login rectangle that types in

“vend0r@email.com” then types in a password below. The “Sign In” CTA button is selected. Text below: The fraudster creates a fake email account.

[Voice-over] Assuming the vendor’s identity, they initiate a request to change the terms or destination of your regular payments.

On screen: An email message fades in the laptop screen with a message containing Bank Name, Routing number and account number. Text below: They request to change the terms or destination of your regular payments.

[Voice-over] The email appears legitimate,

On screen: The entire screen fades while the vendor email is highlighted and scaled up within a white circle. Text below: The email appears legitimate.

[Voice-over] but the new banking information will route all future payments to an account controlled by the fraudster.

On screen: The new fraudster banking information fades into the laptop screen containing available balance and recent transactions. Several money icons swoop across the screen and into the laptop while the available balance increases and several more transactions are added to the fraudsters account. Text below: All future payments are controlled by the fraudster.

[Voice-over] The deception may not be discovered until weeks later when your invoice is past due, leaving you exposed for months.

On screen: The laptop slides off screen to the right while a calendar fades into the center. The calendar months animate quickly from February to April and a circle highlights the Past due date. Text below: Your invoice is past due

[Voice-over] Cyber criminals know the volume of emails you receive is a vulnerable point for your business and they prey on that.

On screen: The laptop scales back and an email inbox fades within including several fake fraud emails. Email icons slide into the laptop from left to right. Text below: The volume of emails you receive is a vulnerable point for your business.

[Voice-over] So how do you protect your company’s assets and reduce your risk of falling victim to business email scams?

On screen: An orange hook slides down in the laptop and grabs an email out of the laptop and let’s go of it as it fly’s to the right of the screen. Text below: Reduce your risk of business email scams.

[Voice-over] Be “Fraud Aware” – follow these best practices.

On screen: The email rectangle lands in the center of the screen, fades to white with new text, “Be Fraud Aware Follow these best practices.”

[Voice-over] Avoid using email for vendor payment changes.

On screen: A large green circle animate in the center of the screen with an email icon. An orange red scales up with X on the bottom right side of the circle. Text below: Avoid using email for vendor payment changes.

[Voice-over] If that’s not possible, implement a two-step verification process:

On screen: The green circle scales back with the number 1 in the center and a dark blue circle slides in next to the green circle with a number 2. Text below: Implement a two-step verification process.

[Voice-over] Call the vendor at a known contact number to confirm the request verbally,

On screen: A phone icon fades into the green circle with a small number 1 below. Text below: Call the vendor at a known contact number to confirm the request verbally.

[Voice-over] or require a second approval.

On screen: A white outlined circle with a green checkmark fades into the blue circle with a small number 2 below. Text below: Require a second approval.

[Voice-over] Never use the phone number or account in the email.

On screen: A hand icon with circles fades into the green circle while a rectangle icon with a green dollar sign fades into the blue circle. A small red circle with an X scales up between the green and blue circles. Text below: Never use the phone number or account in the email.

[Voice-over] Ensure all employees receive fraud awareness training and take the time to validate requests.

On screen: The green circle slides over to the left of the screen with the book icon and the blue circle slides over directly below the green circle with a white outlined circle and green checkmark. Text to the right:
Ensure all employees:
(checkmark) Receive fraud awareness training
(checkmark) Take the time to validate requests

[Voice-over] Provide ongoing education about the dangers of cyber threats and your internal processes for handling these situations.

On screen: A fraud icon fades into the green circle and a rotating gear icon fades into the blue circle. Text to the right:
Provide ongoing education about:
(checkmark) Dangers of cyber threats
(checkmark) Internal processes for handling these situations

[Voice-over] Do everything in your power to keep cyber criminals away.

On screen: A blue lock animates in the center of the screen with animate ones and zeros moving out of it to the right. Text below: Do everything in your power to keep cyber criminals away.

[Voice-over] When the time comes to review your profits, you'll be glad you did.

On screen: Screen fades to white with text in the center: Be Fraud Aware.

[Voice-over] For more fraud prevention tips, visit www.regions.com/stopfraud.

On screen: Text in the center: For more fraud prevention tips, visit www.regions.com/stopfraud.

On screen: Regions logo with disclosures