CORPORATE ACCOUNT TAKEOVER AND CUSTOMER SECURITY AWARENESS

Table of Contents

EFFECTIVE DATE....3
PURPOSE AND SCOPE....3
WHAT CORPORATE ACCOUNT TAKEOVER IS....3
HOW FRAUDSTERS GAIN ACCESS....3
PROTECT....3
DETECT....4
RESPOND....4
HOW TO CONTACT THE BANK....5
ADDITIONAL RESOURCES....5

EFFECTIVE DATE
This customer-awareness document is maintained for 2026 review and distribution in connection with the Bank's online-banking and fraud-awareness program.

PURPOSE AND SCOPE
This program was created to increase our customers' awareness of the potential risks and threats that are associated with Internet and electronic-based services, and to provide solutions and tools to help prevent fraud and scams.

This awareness guide is intended primarily for business customers and other account holders who use online-banking, bill-payment, remote-access, or related digital channels that could be targeted by credential theft, malware, phishing, social engineering, or related account-takeover activity.

WHAT CORPORATE ACCOUNT TAKEOVER IS
Corporate Account Takeover (CATO) is a type of identity theft in which a criminal steals valid online-banking credentials from a business and then uses those credentials to initiate or attempt unauthorized transactions from the account.

Corporate Account TakeOver (CATO) is a growing form of electronic crime where thieves typically use some form of malware, or malicious software, to obtain login credentials to business online banking accounts and fraudulently transfer funds from the accounts. Often these funds may not be recovered.
Current fraud trends may also involve phishing, social engineering, business email compromise, credential theft, device compromise, or attempts to change payees, contact information, security settings, or account-access credentials.

HOW FRAUDSTERS GAIN ACCESS
Fraudsters often attempt to obtain account access by sending emails, text messages, or pop-up messages that impersonate legitimate organizations and direct the recipient to click a malicious link, open an infected attachment, disclose credentials, or approve an unexpected transaction.

Fraudsters also exploit stolen email accounts, spoofed domains, fraudulent phone calls, and urgent payment-change requests to pressure employees into bypassing normal controls.

- Ask for personal or account information.
- Direct the employee to click on a malicious link provided in the email or text message.
- Contain attachments that are infected with malware.
- Impersonate a bank, government agency, delivery company, software provider, executive, customer, or vendor.

PROTECT
Do not respond to or open attachments or click on links in unsolicited emails or messages. If a message appears to be from your financial institution, contact the institution using a trusted phone number or website you already know.
Be wary of pop-up messages claiming your device is infected or that you must install software, approve a one-time passcode, or re-enter credentials.

Use and maintain current anti-virus, anti-malware, spam-filtering, and firewall protections, and promptly install operating-system and application updates.
Conduct online banking and payment activity from a dedicated or otherwise restricted device whenever feasible.

Use strong, unique passwords, do not store passwords on the access device, and enable multifactor authentication or layered security when offered.

Do not use public Wi-Fi or other untrusted networks for online banking unless you have appropriate secure remote-access protections.

Reconcile accounts daily and use dual control or segregation of duties for payment activity whenever possible.

Talk to the Bank about available risk-mitigation services such as alerts, callback procedures, Positive Pay, transaction limits, or other fraud-mitigation tools.

DETECT

Monitor and reconcile accounts at least once each business day and review alerts or exception notices promptly.

Pay attention to warnings from anti-virus, anti-malware, or other security tools.

Watch for unusual system behavior such as dramatic loss of speed, unexpected restarts, new toolbars or icons, unusual pop-ups, inability to log in, or unexpected one-time-passcode requests during a session.

Be alert to unexpected changes to payees, contact information, administrative users, passwords, account settings, or transaction history.

If someone reports receiving a suspicious email from your account that you did not send, or if you find unexplained messages in your sent items, your email may be compromised.

RESPOND

If you detect suspicious activity, immediately cease online-banking activity and disconnect any potentially compromised system from the network.

Immediately contact the Bank so access can be restricted, passwords can be changed, suspicious transactions can be reviewed, and additional protective steps can be taken.

Maintain a written chronology of what happened, what was lost, the actions taken, and the contact information for any person or organization involved in the response.

File a police report when appropriate and consider reporting the incident to the FBI’s Internet Crime Complaint Center (IC3) or other appropriate authorities.

Preserve the affected system and data for possible forensic review before reformatting, rebuilding, or otherwise destroying potential evidence.

Review whether your insurance carrier, card processor, accountant, managed service provider, or other third parties should be notified based on the nature of the incident.

HOW TO CONTACT THE BANK

If you are in doubt about a message, transaction, or payment request, do not use contact information provided in the suspicious communication. Instead, contact the Bank using a phone number from your statement, account-opening materials, or the Bank's official website.

Phone calls and text messages requesting sensitive information are likely fraudulent. Account holders should independently verify the request before taking action.

ADDITIONAL RESOURCES

Specific legacy web links and obsolete resource references were removed and replaced with current official resource names so the document remains maintainable and less likely to contain broken links.

For current guidance, customers may consult the following official resources:

FDIC Cybersecurity Guide for Businesses
CISA small-business and phishing resources
FTC business and consumer fraud resources
FBI Internet Crime Complaint Center (IC3)
NIST small-business cybersecurity resources
Bank of Louisiana customer-security information and fraud-contact guidance

DOCUMENT CHANGE LOG			
Version	**Revision Date**	**Author**	**Description**
1.0	6/22/2026	Vincent J. Maggiore, ISO	2026 review using current BOL documents, Compliance Alliance content, and current regulatory guidance.