RESOURCE BANK

Corporate Account Takeover (CATO) & Fraudulent Transactions

2026 Training

Introduction

- Resource Bank is committed to providing our commercial clients with a **highly sophisticated** level of online protection.
- Unfortunately, in today's digital age, **fraud** is a fact of life.
- All bank departments keep the security of your information in the **highest regard**.
- Our efforts in combination with your **diligence** will set you up for success in preventing a CATO event.

What is Corporate Account Takeover? (CATO)

- Cyber-thieves gain access of a business' bank account & **steal** online banking information relating to the business.
- The most common technique is **malware** infecting a business' computers & laptops.
- This happens through infected **attachments** or **links** via e-mail, websites, social media platforms, and even company networks.
- If the links or attachments are clicked, the malware can install & provide the perpetrator with sensitive banking information such as account numbers and balances.

Compiled by Resource Bank (ELH) 2026
Member FDIC. Equal Housing Lender.

The Rise of Artificial Intelligence: AI

- With the new technologies emerging into main stream daily life, a new threat factor is also being revealed.
- Fraudsters are using **Generative AI** to create “deepfake videos” and clone voices in some cases literally just minutes.
- Tip: The age old saying “**Trust but Verify**” has never been more true then in today’s world. Always use contact information that you already had, not from the communication you just received.
- Creating a sense of urgency and causing panic is going to be a well used tool of the Fraudster.
- Taking the time to **verify** and **authenticate** any request could save you both hours of additional stress as well as thousands of dollars.

Why are Businesses Targeted?

1. They can initiate funds transfers via online banking.
2. Not as many **technological** resources to protect against fraud in smaller businesses.
3. Many do not incorporate systems that regularly monitor accounts (password generation, two-step authentication, etc.).
4. Small businesses usually bank with a **wide array** of financial institutions that may not require these protection services.

As reported by the FBI through IC3

Crime Type:		2024	2025
Business Email Compromise	Loss	$2,770,151,146	$3,046,598,558
	Complaints	21,442	24,768
Tech Support	Loss	$1,464,755,976	$2,134,675,818
	Complaints	36,002	47,794
Investment	Loss	$6,570,639,864	$8,648,617,756
	Complaints	47,919	72,984

FBI Internet Crime Complaint Center
https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

What is Business Email Compromise?

- **Business email compromise** (BEC) is the largest type of Corporate Account Takeover nationally for the last three years.
- This occurs when fraudsters, also known as “bad actors,” hack into a business’ email to attempt to reroute funds being sent electronically. The easiest way for the hacker to gain access to the email account is by tricking the user to click a link within a fraudulent email so they can gain remote access.
- It is important to identify red flags and incorporate best practices.
- Can you identify the Valid email addresses below?

Customersupport@Resource.com or Info@Resource.Bank

Info@Resource.Bank is the valid email

- Can you see the difference between these two email addresses?

INF0@Resource.Bank or INFO@Resource.Bank

Sometimes the difference is as small as the difference between a Zero and a Capital “O”

How Can Financial Institutions Help?

- ❑Integrate **multi-factor** authentication for business accounts.
- ❑Require clients utilize **dual control** (transaction origination & authorization).
- ❑Initiate “out-of-band” confirmations on specific payment types (refers to text, email alerts, etc.).
- ❑Arrange “out-of-band” alerts for uncommon activities.
- ❑Prohibiting credential sharing.
- ❑Authorize & control exposure relating to the clients’ activities.

How Businesses Can Prevent Fraud

- ❑ Utilize **dual control** for payments.
    a) Have one person authorize creation and one authorize release of payment.
- ❑ Confirm that all security & anti-virus software on company computers & laptops are up-to-date.
- ❑ Prohibit shares access
- ❑ Possibly implement second day verification by an employee not involved in initial transaction to prevent internal fraud.
- ❑ Limit the functions of each computer & laptop **strictly** used for online banking
    a) Have a computer for general use that is not connected to internal network.
- ❑ Reconcile banking activity on a **daily** basis.
- ❑ Incorporate alerts for unusual activity.

Compiled by Resource Bank (ELH) 2026
Member FDIC. Equal Housing Lender.

Red Flags and Best Practices

❑Red Flags

a) Bad actor pretending to be the vendor or an employee applies **pressure** to receive payment faster than originally stated.

b) Bad actor changes payment method from check to ACH or from ACH to wire.

c) All communication is being sent via email or fax without verbal verification.

❑Best Practices

a) Any time payment methods or payment information is changed via written communication, a callback should be made to the vendor **directly** with the current contact information already on file with your company.

b) When performing the callback verification, not only confirm the payment method but also that the payment account information is still valid.

If you believe you have become a Victim of Fraud

1. Reach out to relevant law enforcement immediately.
2. Contact **Resource Bank** to initiate an investigation with receiving bank to determine if funds are recoverable.
3. Resource Bank will file appropriate paperwork and keep you informed of the claim status.
4. Take additional steps to evaluate anti virus software is up-to-date on company computers & consider bringing in an outside firm to address and correct any system compromises.

Common Scams

Call Center Scams

Scammers impersonating Cryptocurrency Exchanges or targeting older adults and directing victims to send cash.

Toll Scams

Smishing Scam sent through email or text that looks like money is owed for a Road Toll Service

Emergency Scams

Telephone Scam that convinces a victim that a relative is in financial or legal crisis. This scam typically uses AI to mimic the voice or physical appearance of the relative which gives legitimacy to the scam.

Additional Resources

- FFIEC

http://www.ffiec.gov/pdf/authentication_guidance.pdf

- FDIC

https://www.fdic.gov/

- FBI

https://www.fbi.gov/contact-us/field-offices

- FTC

http://ftc.gov/redflagsrule

- Internet Crime Complaint Center

http://www.ic3.gov/

- Financial Services

http://www.fsisac.com/

Questions?

CashManagement@resource.bank | 985.801.0120

Or send a secure message from within the online banking portal.

We appreciate your business and referrals.

RESOURCE BANK