



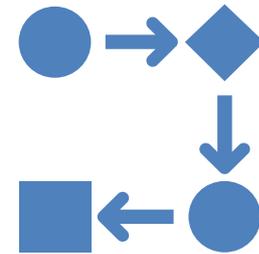
# Wire Fraud in Local Government Projects: Lessons from Chetek

A story of how one city  
responded, and what others can  
learn.

# A Normal Day... Until It Wasn't



On my first day, it felt like  
business as usual.



Behind the scenes,  
something wasn't right...

# The Incident

September 19, 2023 - 1:45 pm email Patrick Sullivan (Market & Johnson) and Chad Ellingson (CBS Squared) and CC'd Chad Ellingson (Market & Johnson) and Tia McCarthy (CBS Squared) regarding a payment that was due on August 30th. (email addresses appear to be spoofed). Tia McCarthy replied at 2:52 stating AFP #4 was delayed.....and that they were processing AFP #4 with AFP #5. Cc'd Chad Ellingson (Market & Johnson) and John Sworski (CBS Squared).

Patrick replied back at 2:57 pm - thanks for the update - cc'd Chad Ellingson, John Sworski as well.

9/19/23 - 9:58 pm  
Chad Ellingson (market & johnson) emailed Patrick Sullivan (market & johnson) & Tia McCarthy (cbs squared) and cc'd John Sworski (cbs squared)

Asking Tia for clarity on the estimated payment date for the two AFPs

September 20th - 9:08 AM - Tia McCarthy replied to the 9/19 email to Chad Ellingson, Sullivan and John Sworski - advising the City will be wiring funds today.

September 20th - 3:21 PM - Chad Ellingson (phishing email) sent to Tia mccarthy, Patrick Sullivan (phishing email) and John Sworski - to confirm that they will be receiving the pay and that their banking information has changed.

At 3:28 - Tia McCarthy emailed me and cc'd John Sworski, Chad Ellingson (phishing email) and Patrick Sullivan (phishing email) "putting you in contact with Market & Johnson regarding AFP payment.

At 3:38 - email to Carmen Newman received from Chad Ellingson (phishing email) & cc' John Sworski & Patrick Sullivan (phishing email) - asking me to advise on the email being (referring to the email he sent to Tia McCarthy).

9/20/23 - 4:10 pm - Carmen Newman emailed the phishing emails advising the funds were wired for AFP #4 & 5.

9/21/23 - email from Chad Ellingson (phishing email) "payment received - thanks" is payment did actually go to the correct account for Market & Johnson

October 2, 2023  
Carmen Newman from Chad Ellingson (phishing email) advising payment was made to Britany Gerth, Patrick Sullivan - all phishing emails and

October 2, 2023  
Carmen Newman from Chad Ellingson (phishing email) advising payment was made to Britany Gerth, Patrick Sullivan - all phishing emails and



**Account Name:**  
Market & Johnson

2350 Galloway St.  
P.O. Box 630.  
Eau Claire, WI  
54702-0630

**Citi Bank**

4395 N Town Hall  
Rd Eau Claire, WI  
54703

**ROUTING#** 271070801  
**ACCOUNT#:** 802085087

October 17, 2023  
Funds were wired to Market & Johnson (fraudulent account) through Sterling Bank. The funds went to the Citibank account. (incorrect account)

November 14th - received email from Tia McCarthy regarding AFP #7- cc'd to CBS squared staff, chetek mayor, and Dan Knapp (public works director)

November 15th -  
Email from Patrick Sullivan to Tia McCarthy asking about payment for AFP #6  
Email to Carmen Newman from Tia McCarthy (cc'd Patrick Sullivan - correct email, Dan Knapp and Britany Gerth - Market & Johnson - correct email) asking about the wire for payment AFP #6  
November 16th - Carmen Newman emailed the above stating wire was sent on 10/17 and I would check with bank in the am.

November 16th - notified Sterling Bank, Jeff Martin, Dan Knapp, Ron Ambrozaitis (police chief Mark Meeks-W3 insurance regarding wire fraud. Sterling Bank notified FBI, police chief not county sheriff. Carmen Newman contacted Market & Johnson and CBS Squared. Carmen spoke to Linda Armstrong (cbs squared IT person). She advised that antivirus software was removed from John Sworski computer and moved off of Microsoft license. Linda Armstrong advised she did not find they were compromised.

November 17th - Market & Johnson - Chad & Patrick called advising they were hiring analysts.

November 21, 2023 - Anthony Forde (Kivu forensic analyst) connect to our computer to check for any compromise. He didn't find any malicious activity or notification obligations.

November 21, 2023 - received another phishing email from (chad ellingson) cc'd to Britany Gerth, Patrick Sullivan and Tia McCarthy - all phishing emails and

- In November 2023, Chetek fell victim to wire fraud.
- \$2.6 million was sent to a fraudulent account.
- Fortunately, the funds were later recovered.

## How It Happened

Fraudsters spoofed contractor emails.

Fake payment instructions were sent.

The City believed the instructions were legitimate.

# Discovery & Response

- Alerted banks, FBI, state and local law enforcement.
- Paused financial transactions immediately.
- Engaged forensic experts to verify systems.

## CHANGE ORDER REQUEST (COR)

TO: City of Chetek  
220 Stout Street, PO Box 194  
Chetek, WI 54728

DATE: March 15, 2024

RE: Change Order Request (COR) #27  
3255 - Chetek Wastewater Treatment Facility  
698 County Highway SS  
Barron County, WI 54728

ATTN: Jeff Martin

DESCRIPTION OF CHANGE: Forensic Analysis for Our Server System

REQUESTED BY WHOM:

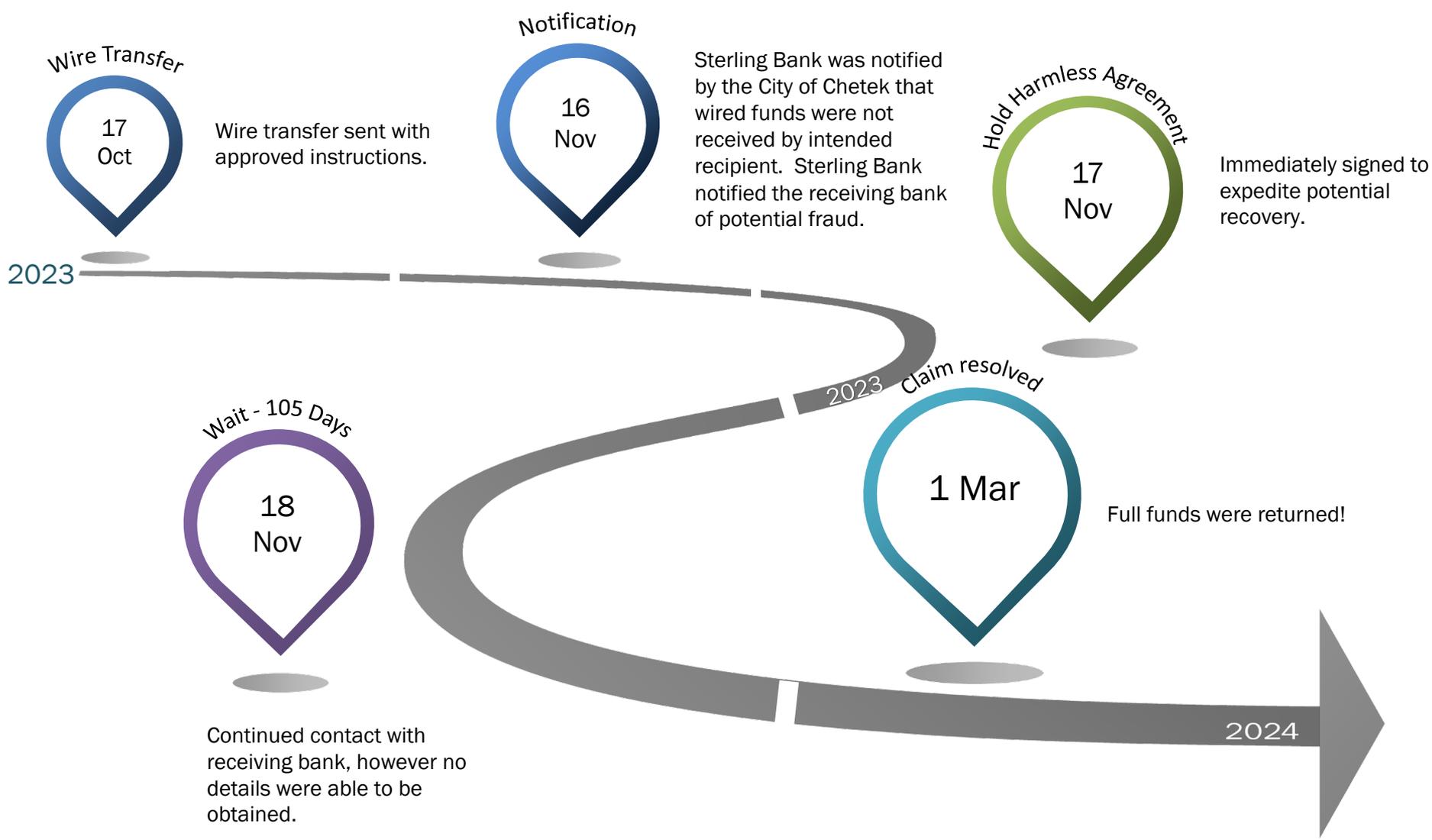
COST OF WORK:  
Changes to Market & Johnson's Scope of Work (see attached breakdown) ..... \$33,289.00  
**TOTAL CHANGE TO PROJECT** **\$33,289.00**

TIME: The Contract Time will be unchanged by zero days for this change.

INSTRUCTIONS RECEIVED:

# What did Sterling Bank do?

- Contacted receiving bank through multiple avenues
  - Electronically
  - ABA Fraud Contact Directory contacts were also utilized
    - Phone, email, and mail contacts
- Sterling Bank signed a Hold Harmless Agreement
- Contacted the FBI



# Importance of a Community Bank

Sterling Bank suffered no financial loss. They relied on approved wire transfer instructions. So why help?

**Sterling Bank approached it as a partnership with their customer**

**The impact to the City impacts the entire community**

**Sterling Bank was able to bring additional resources to utilize**

# Lessons Learned



VERIFY WIRE TRANSFERS  
WITH A PHONE CALL.



REQUIRE TWO-PERSON  
APPROVAL FOR LARGE  
PAYMENTS.



TRAIN EMPLOYEES TO  
SPOT PHISHING ATTEMPTS.

# What You Can Do in Your City

- Don't assume it can't happen to you.
- Build fraud prevention into contracts.
- Establish response protocols before an incident.
- Connect with FBI and state partners now.

[www.citibank.com](http://www.citibank.com)

Re: 802085087  
Dear STERLING BANK,  
Your claim dated 02/07/2024 for \$2,680,472.00

**Why We're Writing to You**

**What You Need to Know**

- Has been honored. Please see attached check number 892161977 in the amount of \$2,880,472.00.

**How To Contact Us**

If you have any questions or would like to speak with a fraud representative, they may be contacted toll-free Monday – Friday, 9:00 a.m. to 5:30 p.m. ET at:

- Toll Free 1-833-782-1456 Letter Code: 7070
- International Calls 1-210-677-0085
- For TTY: We accept 711 or other Relay Service
- The number on the back of your Citibank Banking Card

For your convenience any further claim correspondence can be forwarded via fax or mail to:

- Fax #: 1-210-547-9176
- Mail: CITIBANK N.A.  
Fraud Prevention  
P.O. Box 769027-0027  
San Antonio, TX 78245-9963

Sincerely,  
Citibank Fraud Prevention

Calls are randomly monitored and recorded to ensure quality service.  
Please consult the Citibank Client Manual- Consumer Accounts for important conditions and limitations.  
Fraud Control & Risk Management performs risk management functions for Citibank, N.A.  
©2024 Citibank, N.A. Member FDIC. Cit, Private Pass and Cit with Arc Design are registered service marks of Citigroup Inc. All rights reserved.

# Closing & Discussion

- Fraud can happen to any city.
- Swift action + prevention policies are key.
- Questions & discussion.

