Don’t Gamble with Business Payments: Averting ACH Fraud and Check Fraud

Steven Bott, CPA
Managing Supervisor, Treasury Technology Services
Ameren Corporation

Lucy Suarez, CTP
Senior Solution Consultant
ACI Worldwide

Greg Litster
President
SAFEChecks
## Overview from the Corporate Perspective: Ameren Risk and Exposure - ACH

<table>
<thead>
<tr>
<th>Category</th>
<th>Transactions</th>
<th>Dollars</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable</td>
<td>106,000</td>
<td>$4,724,000,000 ($4.7 Billion)</td>
<td>$44,600</td>
</tr>
<tr>
<td>Payroll</td>
<td>314,000</td>
<td>$697,000,000</td>
<td>$2,220</td>
</tr>
<tr>
<td>Customer Refunds</td>
<td>0</td>
<td>$0</td>
<td>$0</td>
</tr>
</tbody>
</table>
## Checks

<table>
<thead>
<tr>
<th>Category</th>
<th>Transactions</th>
<th>Dollars</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable</td>
<td>37,000</td>
<td>$779,000,000</td>
<td>$21,100</td>
</tr>
<tr>
<td>Payroll</td>
<td>400</td>
<td>$1,330,000</td>
<td>$3,300</td>
</tr>
<tr>
<td>Customer Refunds</td>
<td>105,000</td>
<td>$30,000,000</td>
<td>$286</td>
</tr>
</tbody>
</table>
Annual Fraud Attempts Against Bank Accounts (2013)

- Number of attempts: 75
- Total dollars of attempts: $165,000
- Average transaction: $2,200
- Customer Refund Account Targeted
Types of Fraud Attempts

- **Ameren Illinois** Customer Refund Account
- **Check #177249** issued January 4, 2013: $104.00
Types of Fraud Attempts

• **Ameren Illinois** Customer Refund Account
• Check #177241 issued January 4, 2013: $342.10
• **Logo changed** to Ameren **Missouri** – Payee address is in Missouri
Types of Fraud Attempts

- Seller on Craigslist receives fraudulent check higher than purchase price.
- "Buyer" asks to send back over-amount – Seller out the cash and item sold
Types of Fraud Attempts

• Payment for Services - Receiver of check told he would be paid for allowing "Ameren" to wrap his truck with advertising

  – They send a check for too much. Request that he send back the difference

  – Classic scam that can lead to Holder In Due Course claims

• Lottery Scams
Types of Fraud Attempts
Fraud Prevention Controls in Place

- **Checks:**
  - Payee Positive Pay
  - Separate bank accounts where possible
  - No check service
  - List check stock controls

- **ACH:**
  - Debit blocks
  - ACH Positive Pay Service

- Notify bank of fraud attempts to place alert on account for teller reference
Convert Checks to Electronic

• Payroll – Incorporated ACH Direct Deposit requirement into labor agreements. Mandated for management employees.

• A/P – Moved transactions to credit card or ACH

• Refund checks – haven’t yet moved to electronic payment, but are planning to do so
A Closer Look at ACH Fraud

Lucy Suarez, CTP
Senior Solution Consultant
ACI Worldwide
Agenda

• Volume and type of ACH
• Types and examples of fraud
• Industry statistics
• Ways to mitigate fraud
  – Financial Institutions
  – Corporate Practitioners
# ACH Volume 2nd Quarter 2013

<table>
<thead>
<tr>
<th></th>
<th>2nd·Qtr·2013</th>
<th>1st·Qtr·2013</th>
<th>% Change</th>
<th>2nd·Qtr·2012</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARC</td>
<td>430,490,891</td>
<td>442,270,070</td>
<td>-2.66%</td>
<td>467,558,353</td>
<td>-7.93%</td>
</tr>
<tr>
<td>BOC</td>
<td>44,579,560</td>
<td>42,997,063</td>
<td>3.68%</td>
<td>48,630,940</td>
<td>-8.33%</td>
</tr>
<tr>
<td>CCD-Debits</td>
<td>198,361,199</td>
<td>187,296,563</td>
<td>5.91%</td>
<td>183,992,499</td>
<td>7.81%</td>
</tr>
<tr>
<td>CCD-Credits</td>
<td>412,984,763</td>
<td>389,018,959</td>
<td>6.16%</td>
<td>390,176,833</td>
<td>5.85%</td>
</tr>
<tr>
<td>CIE</td>
<td>44,075,437</td>
<td>44,170,426</td>
<td>-0.22%</td>
<td>41,433,173</td>
<td>6.38%</td>
</tr>
<tr>
<td>CTX</td>
<td>23,892,524</td>
<td>22,443,814</td>
<td>6.45%</td>
<td>21,567,562</td>
<td>10.78%</td>
</tr>
<tr>
<td>IAT</td>
<td>11,594,718</td>
<td>11,194,487</td>
<td>3.58%</td>
<td>10,830,572</td>
<td>7.06%</td>
</tr>
<tr>
<td>POP</td>
<td>104,264,353</td>
<td>99,420,798</td>
<td>4.87%</td>
<td>117,349,000</td>
<td>-11.15%</td>
</tr>
<tr>
<td>PPD-Debits</td>
<td>800,307,133</td>
<td>789,646,749</td>
<td>1.35%</td>
<td>767,281,866</td>
<td>4.30%</td>
</tr>
<tr>
<td>PPD-Credits</td>
<td>1,336,890,746</td>
<td>1,365,542,800</td>
<td>-2.10%</td>
<td>1,270,656,562</td>
<td>5.21%</td>
</tr>
<tr>
<td>RCK</td>
<td>1,069,472</td>
<td>1,162,073</td>
<td>-7.97%</td>
<td>1,413,038</td>
<td>-24.31%</td>
</tr>
<tr>
<td>TEL</td>
<td>91,052,333</td>
<td>92,090,383</td>
<td>-1.13%</td>
<td>84,005,473</td>
<td>8.39%</td>
</tr>
<tr>
<td>WEB</td>
<td>806,182,262</td>
<td>790,254,489</td>
<td>2.02%</td>
<td>718,403,310</td>
<td>12.22%</td>
</tr>
<tr>
<td>Others</td>
<td>42,804,296</td>
<td>39,489,290</td>
<td>8.39%</td>
<td>29,776,146</td>
<td>43.75%</td>
</tr>
<tr>
<td>Total-Network</td>
<td>4,348,549,687</td>
<td>4,316,997,964</td>
<td>0.73%</td>
<td>4,153,075,327</td>
<td>4.71%</td>
</tr>
</tbody>
</table>
NACHA defines fraud risk as:

“the risk that ACH data will be compromised through the introduction of false transactions, the alteration of valid transactions, or the alteration of static data that controls the routing or settlement of valid ACH transactions.”
Danger lurks….

- Payroll checks
- Shady telemarketers
- Even NACHA!!!!!
Fraud and Loss

• 61% had attempted or actual payment fraud
  – 27% had attempted or actual ACH debit fraud, UP FROM 23% IN 2012!
• 45% had potential loss < $25k
• 73% had no actual loss

Source: 2013 AFP Payments Fraud Survey
Fraud Makes Headlines

ACH liability up for grabs as court finds against bank in second US cyber-heist suit

A Michigan court has found in favour of Experi-Metal in its $560,000 cyber-heist suit against Comerica Bank, contradicting a ruling last week in a separate small business ACH fraud case which came down on the side of the bank.

In the Experi-Metal case, Judge Patrick Duggan of the US District Court for the Eastern District of Michigan said that the bank should have done a better job of picking up the fraudulent transactions running from the company’s accounts after its financial controller was duped into opening a malware-laden phishing e-mail.

In summing up, Duggan said “a bank dealing fairly with its customers, under these circumstances, would have detected and/or stepped the fraudulent wire activity earlier.”

Who Bears Online Fraud Burden: Bank Or Business?

Two recent court cases with very different outcomes call attention to the uncertain—and potentially expensive—environment for online banking security.

By Kevin Casey InformationWeek
June 27, 2011 01:30 AM

Financial institutions have your back if hackers steal your business’s money. Right? Don’t bank on it. Two recent lawsuits highlight the murky online security waters that smaller businesses wade in with their banks, and show that SMBs can’t rely too heavily on their banks for protection against account fraud.

New ACH Fraud Suit Filed

Village View Escrow is Latest Fraud Victim to Sue Bank

By Tracy Kitten, July 13, 2011

A March 2010 incident of corporate account takeover has led to yet another legal fight between Village View Escrow Inc. and its former bank. [The bank] filed a lawsuit against Village View Escrow Inc., which was then a California-based real-estate escrow company.

Yet Another Bank Sued By A Small Business For Fraudulent Hacker Transfers

According to Village View, Professional Business Bank says bank responsible for $465K loss to hackers, plus fees and damages suffered in online account breach

Jul 19, 2011 | 10:34 PM | 1 Comments

By Ericka Chickowski, Contributing Writer

A new court case brought to bear against Professional Business Bank by Village View Escrow Inc. continues the battle waged over who’s to blame for hacking attacks that leave small-business accounts drained following online password theft. Filed in late June in the California Superior Court in Los Angeles, the case is the latest in a string of lawsuits filed in U.S. courts by small businesses that believe their banks are to blame for failing to properly protect their accounts from predatory hackers.
Financial Institutions should...

- Educate Employees
- Customer education and training (FFIEC requirement)
- Set transaction limits
- Implement risk applications
- Offer fraud mitigation products
Phishing Attacks

Fraudulent Email Example 1
(subject lines vary, random number generation, cancelled, rejected, denied)

Subject: ACH Payment 3396043 Cancelled

Payment Notification # 3356941

The ACH Transaction (ID:33456941), recently initiated from your checking account (by you or another person) was cancelled by the other financial institution.

Rejected transaction ID:33456941
Reason for Rejection: See details in the attachment.
Fraud Alerts

- E-Mail and Facebook phishing scams in relation to Boston Marathon Explosion
  The US Department of Homeland Security has issued a warning about an influx of scams in relation to the Boston Marathon explosion. The intense public interest in the event has created the groundwork for scammers looking to exploit consumers.

- Fraudulent Fax/Wire Scheme
  At this time we want to educate our customers of a potential facsimile (fax) claiming to be from The US Department of Transportation. We have received reports that individuals and/or companies have received a fraudulent fax that has the appearance of having been sent from The US Department of Transportation.

- Phishing Alert - Intuit Quickbooks
  At this time we want to educate our Online Banker users of a potential e-mail claiming to be from QuickBooks. Intuit has received reports that individuals and/or companies have received a fraudulent e-mail that has the appearance of having been sent from Intuit.

- Automated Phone Message Alert
  It has been reported that there are automated phone message attempts targeting bank customers. These voice phishing attacks are often referred to as “vishing.” The call will be a pre-recorded phone message delivered to random consumers with the warning that their debit cards have been closed, “reached their max limit”, “blocked” or “deactivated”.

- New E-Mail and Facebook Zeus Malware Trojan Warning
  At this time we would like to advise all customers about a new fraud trend being aimed at Yahoo, Google Mail, Hotmail & Facebook users. These malicious offers come disguised as chance for a great “rebate” or “new security functionality.”

- Important Reminder Regarding Internet Account Takeover
  E-mail and Internet-related fraudulent schemes, such as “account takeover” are being perpetrated with increasing frequency, creativity and intensity. Account Takeover is a form of corporate identity theft where a business’ online credentials are stolen by malware or viruses.

- Masquerading Website Alert
  It has been brought to our attention from the Office of the Comptroller of the Currency (OCC) that there are malicious attempts to redirect consumers to an illegitimate website.
ACH Fraud Controls

• 38% Block ACH debits on all accounts

• 41% Block all ACH debits on a single account setup with ACH debit filter/ACH Positive Pay

• 28% Debit block on all consumer items with debit filter on commercial ACH debits

Source: 2013 AFP Payments Fraud Survey
Corporate Practitioners should…

- Implement Dual Control
- Separate accounts
- Separate Duties
- Strong Passwords
- Use a specific PC to log onto the bank
- Perform daily reconciliation
- Update antivirus
- Be aware of small dollar transactions
Man-in-the-Browser (MITB) Attack

What I see....

What the MITB sends....
Everyone is learning to love ACH – including the crooks!
Check Fraud

Greg Litster
President
SAFEChecks
Check Fraud

Why talk about Check Fraud?
Check Fraud

Produces more $ Losses

than all other types of payment fraud

COMBINED!
In 1492...

Columbus Sailed the Ocean Blue!
In 1762...

Price sued Neal for check fraud

Price v. Neal, England

(The FIRST Check Fraud Lawsuit)
Check fraud has continued unabated for 250 years!
In 2013
with 70% of organizations
still issuing checks,
check fraud will never go away!
"Checks remain the most popular vehicle for criminals committing payments fraud, even though the corporate use of checks has declined."

AFP 2013 Payments Fraud Survey
Total Non-Cash Payments by Method (Transactions)

2010 Federal Reserve Payments Study
(the next study will be released at the end of 2013)
Fraudulent Payments by Method
(Respondents were hit multiple ways; total > 100%)

- CHECKS 87%
- Purchasing Cards 29%
- ACH Debits 27%
- Wire Transfer 11%
- ACH Credits 8%
Fraud Losses by Method

How Dollars were actually lost

- Checks: 69%
- Purchasing Cards: 10%
- ACH Debits: 9%
- ACH Credits: 7%
- Wire Transfer: 5%
Frank Abagnale

*Catch Me If You Can*

Technology is making Frank Abagnale’s “gift” achievable by mere mortals
Boston’s #1 Seller
The Evolution of Check Fraud and Banker Solutions
Counterfeit Checks
(since 1762)

...Banks developed Positive Pay
Altered Payees

...Banks developed Payee Positive Pay
Added Payee Names

Checks blow right through Payee Positive Pay!
Typical Check Layout

Open Areas Where Forgers Add A New Payee Name

Added Payee printed 2 lines above original name will not be detected by Payee Positive Pay
Multiple Payees:

If it doesn’t say **AND**, it is “ambiguous” and legally means “**OR**”.

A forward slash [virgule, vər-gyül “/” ] = **OR**
Strategies to Prevent Check Fraud
Don’t Write Checks!

• Use Commercial Purchase Cards
• Pay electronically (ACH)
1. Reduces check writing and check fraud risk
2. Does not expose the checking account number
3. Terminating a card is easier than closing a checking account
4. Reduces bank per-item fees
5. Potential for Rebates or Rewards
ACH Payment Benefits

1. Reduces check writing and check fraud risk
2. Does not expose the checking account number
3. Reduces mailing expense and bank fees
4. Pay 1 invoice at a time, or
5. Pay multiple invoices and email remittance detail
If you’re going to write checks...
#1. High Security Checks
Effective check fraud prevention strategies begin with a high security check.
AFP 2013 Payment Fraud Survey

Types of **Attempted** or **Actual** Check Fraud Events:

1. Counterfeit Checks = 66%

2. Altered Checks = 34%
Types of Attempted or Actual Check Fraud Events:

1. Payee Name Alterations = 49%
2. Dollar Amount Alterations = 28%
3. Payee + Dollar Alterations = 23%
High Security Checks

1. Thwart forgers’ attempts to replicate or alter the check

2. Deter the forger (psychological warfare)

3. Provide legal protection from some Holder in Due Course claims (UCC § 3-302)
What makes a check secure?

10+ safety features
Important Security Features

- **Controlled** Check Stock
- Dual-tone True Watermark
- Thermochromatic Ink (reacts to heat)
- Warning Bands worded correctly
- Toner Anchorage
- Copy Void Pantograph
- Chemical-reactive Ink + Paper
- Inventory Control Number on Back (laser)
- UV Ink + UV Fibers
- Microprinting
- Laid Lines

www.safechecks.com
Controlled Check Stock

- Is a critical security feature

- Checks should be unique in some way to every other organization’s check stock

- No two organizations should have the exact, identical check stock

www.safechecks.com
Uncontrolled Check Stock

- Is NOT uniquely designed or customized for each end-user
- It is often sold entirely blank to countless entities / organizations, and fraudsters, by print brokers all over the USA

www.safechecks.com
Who Sells Blank, Uncontrolled Checks?

- Virtually ALL accounting / check writing Software Vendors

- Virtually ALL check printers
  1. Large, national printers
  2. Small print brokers that buy from wholesalers
Ask your check supplier this question:

Has your check stock ever been sold entirely blank to other companies?
Obtain **Controlled** Check Stock

1. **Custom-manufacture** checks using an ORIGINAL design, true-watermarked paper, and at least 10 security features, **OR**

2. **Buy from a supplier** that sells **controlled** check stock that has not been replicated or used in a check fraud scam, ever.

SAFEChecks.com

AFP® Annual Conference

Association for Financial Professionals®
#2. Payee Positive Pay
Positive Pay...

...a powerful tool!

PositivePay.net
Provides **NO PROTECTION** Against
Provides NO PROTECTION Against

Added Payee Names
Lawsuit

Cincinnati Insurance Company

v.

Wachovia Bank

$154,000 Loss from an Altered Payee
CINCINNATI INSURANCE COMPANY v. WACHOVIA BANK, NATIONAL ASSOCIATION
CASE NO. 08-CV-2734 (PJS/JJG).

CINCINNATI INSURANCE COMPANY, as Subrogee of Todd's Snax, Inc., d/b/a Schultz Foods Company, Plaintiff,
v.
WACHOVIA BANK, NATIONAL ASSOCIATION, Defendant.

United States District Court, D. Minnesota.
July 14, 2010.
Prior to the $154,000 loss, Schultz Foods had three (3) separate check fraud events.

Wachovia Bank covered their losses; told Schultz to use Positive Pay or close their account.

Each time Schultz closed their account, but never implemented Positive Pay.
Facts

Schultz buys check fraud insurance from Cincinnati Insurance.
Facts

Schultz Foods issues $154,000 check payable to Amerada Hess Corporation.

Check is stolen.

Payee Name altered, changed to “Kenneth Payton”

Kenneth Payton, a minister, deposits $154,000 check into TCF Bank and wires $150,000 to Singapore to help a South African refugee family.

Wachovia pays the altered check; TCF Bank is liable.
6 weeks later, Schultz Foods notifies Wachovia of altered payee; demands repayment from Wachovia.

Wachovia refuses to pay until it recovers $ from TCF.

Schultz files a claim with Cincinnati Insurance; Cincinnati pays the claim and sues Wachovia.

Under UCC § 3-119, TCF Bank (the liable party) hires attys to defend Wachovia, using Wachovia’s signed “deposit agreement” against Cincinnati Insurance.
Wachovia’s Deposit Agreement (Contract)

“You agree that if you fail to implement any of these products or services, or you fail to follow these and other precautions reasonable for your particular circumstances, you will be precluded from asserting any claims against [Wachovia] for paying any unauthorized, altered, counterfeit or other fraudulent item that such product, service, or precaution was designed to detect or deter, and we will not be required to re-credit your account or otherwise have any liability for paying such items.”
Because of the signed deposit agreement,

Wachovia Bank Wins!

This case demonstrates you can have a great relationship with your bank and still lose a lawsuit!
Fact

If Schultz Foods had used Positive Pay, the check may not have paid and there may not have been a loss!
If Schultz Foods had used Positive Pay, the check may not have paid and there may not have been a loss!

(Exception: Added Payee Names)
Preventing Altered Payees

- High-security checks
- 14 point font for Payee Name
- High-quality toner
- Hot laser printer
- Payee Positive Pay

Frank Abagnale’s Fraud Bulletin on Laser Check Printing
What about **Added** Payee Names?

**It. Is. A. Fact:**
Payee Positive Pay systems are not detecting **Added Payee Names**
printed 2 lines above the original payee name.

There is NO banker solution!
Typical Check Layout

Open Areas Where Forgers Add A New Payee Name
Fix it: Use a Secure Name Font
Leaves No Room for Adding Bogus Payee
Deterrence: Encrypted barcode
Barcode contains:

1. Drawer
2. Payee Name
3. Dollar Amount
4. Issue Date
5. Check Number
6. Account Number
7. Routing/Transit Number
8. Date and Time Check was printed
9. Laser Printer used
10. The employee that printed the check
Holder in Due Course

Web: FraudTips.net
Holder in Due Course

- An innocent party who accepts a check for goods or services
- No evidence of alteration or forgery, or knowledge of fraud by recipient

- **Statute of Limitations**
  - 10 years from date of issue
  - Three (3) years from date of return

- **A Holder in Due Course can sell his/her rights**
Holder in Due Course

- Trumps Stop Payments
- Trumps Positive Pay

Trump (n.) To get the better of an adversary or competitor by using a crucial, often hidden resource.
Holder in Due Course

- Contacted Once: 22%
- Contacted 2 - 10 Times: 66%
- Contacted More Than 10 Times: 12%
Holder in Due Course

- Paid Full Value Of Check Or More: 53%
- Did Not Pay: 47%
- Still In Dispute: 27%
- Other: 7%
Holder in Due Course
Federal Appellate Court
Lawsuits
Robert Triffin v. Somerset Valley Bank and Hauser Contracting Company

- 80 counterfeit checks totaling $25,000 on authentic-looking check stock (looked like ADP payroll checks)
- Bank catches many, and returns them as counterfeit
- Triffin buys $8,800 in returned checks from four check cashing stores, and as a HIDC, sued Hauser for NEGLIGENCE for not controlling his checks.

HIDC & Controlled Check Stock

- Lower court rules in favor of Triffin, saying the checks looked “genuine”
- Hauser appealed; claimed he never had possession of the checks or authorized their issuance.
- Federal Appellate Court UPHELD lower court; also ruled the checks looked “genuine”
- Hauser Contracting ordered to pay Triffin $8,800

Solution: Use controlled, high security checks

HIDC & Stop Payments

Robert Triffin v. Cigna Insurance

- Two year old check; payment stopped
- No “expiration date” printed on check
  - UCC: Check valid for 10 years or 3 years
- Print on checks: “This check expires and is void 25 days from issue date”
  - Don’t re-issue check until first check expires

Someone who accepts an expired Instrument Has No Legal Standing!

Has No Legal Standing!

As a Holder in Due Course
Choice Escrow and Land Title

vs.

BancorpSouth Bank

Important Link

March 17, 2010: Bank received an internet-based request to wire $440,000 out of Choice Escrow’s Trust Account

Request not legitimate – Choice Escrow employee’s computer was hacked, taken over by fraudsters

NO “Dual Authentication” in place at Company

Wire transfer request to send $440K to Republic of Cypress

Computer Takeover:  **NO** “Dual Control”

- Wire to Cypress was initiated using the User ID and password of a Choice Escrow employee.
- Wire was initiated from IP address registered to Choice.
- Bank authenticated employee’s computer by detecting the secure device ID token that Bank previously installed.
- Immediately after wiring funds, Bank auto-generated a Transaction Receipt that was faxed to and received by Choice Escrow. Fax placed on a desk, without review.
Bank: Customer Failed to Implement “Dual Control”

✓ Bank required online banking customers sending wires to utilize “Dual Control”

✓ Dual Control = 2 computers, 2 logins, 2 passwords

✓ Wire transfer could only be effectuated by two individuals using separate User IDs and passwords

✓ Choice declined in writing, TWICE, to use Dual Control
Choice contended “Dual Control” was not “commercially reasonable” because…

“…at times, one or both of the two individuals authorized to perform wire transfers through the [bank] system were out of the office due to various reasons.”

Court disagreed.

Choice Escrow held liable for loss.
Official Comments to the Funds Transfers provisions of the UCC:

The purpose of having a security procedure deemed to be commercially reasonable is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud.

A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available.
For the foregoing reasons, the Court GRANTS the MOTION OF DEFENDANT BANCORPSOUTH FOR SUMMARY JUDGMENT. All other pending motions, including all other motions for summary judgment (including motions for partial summary judgment), are DENIED as moot. Accordingly, it is ORDERED that summary judgment is entered in favor of defendant BancorpSouth Bank."
Prevent Online Banking Fraud

Require 2 different computers to move $$

1. Computers #1-99 can “originate” wires

2. Dedicated “banking-only” computer to “release” the wire / ACH
Greg Litster, President
SAFEChecks
8934 Eton Avenue
Canoga Park, CA  91304

Email: GLITSTER@aol.com
greg@safechecks.com

Phone: (800) 949-2265 direct
Lucy Suarez, CTP  
Senior Solution Consultant  
ACI Worldwide  
123 Main Street  
New York, NY 11111  
(718) 227-2868  
lucy.suarez@aciworldwide.com
Steven Bott, CPA
Managing Supervisor, Treasury Technology Services
Ameren Corporation
1901 Chouteau Avenue
Saint Louis, MO 63103
(314) 554-4306
SBott@ameren.com

• Leads Ameren’s Treasury Technology Services team, previously led Accounts Payable
• Member of AFP and St. Louis Treasury Management Association.

Ameren Corporation
• Fortune 500 company with assets of $23 billion.
• Serves 2.4 million electric customers & over 900,000 natural gas customers across Illinois & Missouri.
• Employs more than 9,000 people.