Commerce Bank™
Member FDIC

Understanding Payments Fraud

November 1, 2017

The Oklahoma Society of CPAs - Tulsa Chapter

Presenters: Commerce Bank & GableGotwals

Agenda

- Evolution of Banking
- Fraud Statistics
- Examples of Payments Fraud
- Fraud Prevention Tools
- Best Practices
- Combating Cyber Crime

About Commerce Bank

150+

Years in the Industry

39th

Largest U.S. Bank[3]

7th

Largest Purchasing Card Issuer[1]

5th Generation

of Management by Kemper Family

4,727

Employees as of 12.31.2016

Moody's Highest Rating

Among Top 7

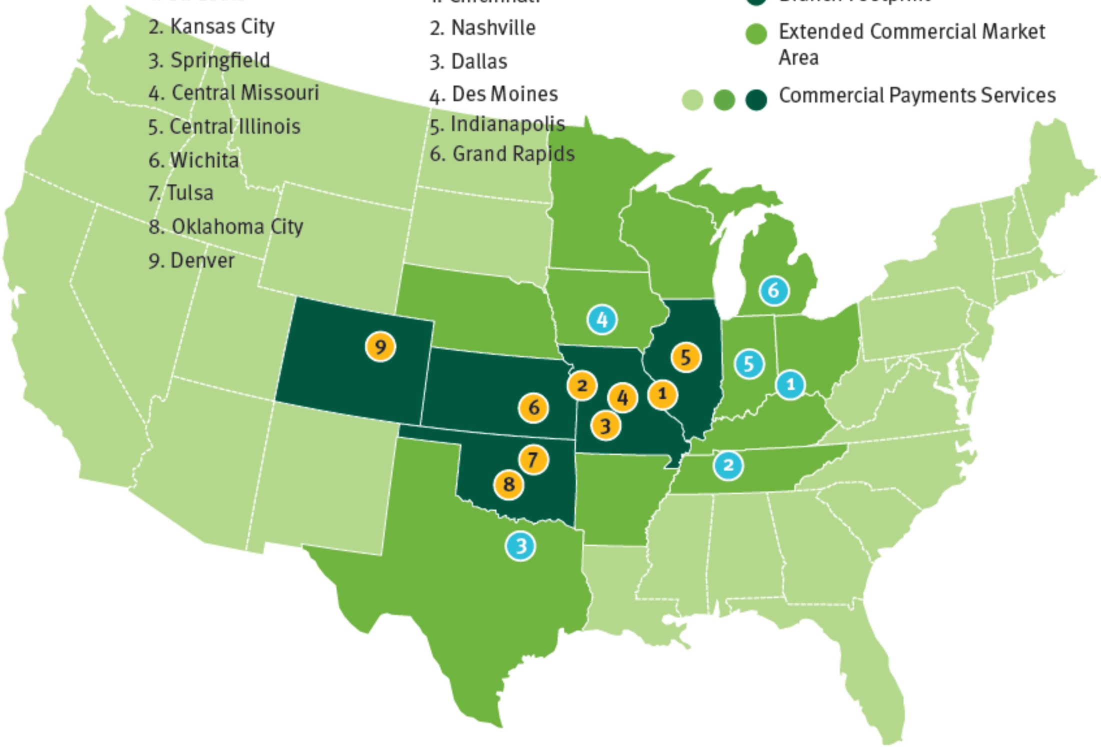
Banks in the Country[2]

$25.6B

In assets as of 12.31.2016

[1] Nilson Report, June 2016, #1089
[2] Moody's Investor Services, Inc., November 15, 2016
[3] SNL Financial ; ranking as of September 30, 2016

Our Footprint



● **NINE KEY MARKETS**

1. St. Louis
2. Kansas City
3. Springfield
4. Central Missouri
5. Central Illinois
6. Wichita
7. Tulsa
8. Oklahoma City
9. Denver

● **COMMERCIAL OFFICES**

1. Cincinnati
2. Nashville
3. Dallas
4. Des Moines
5. Indianapolis
6. Grand Rapids

COMMERCE US PRESENCE

● Branch Footprint

● Extended Commercial Market Area

● ● ● Commercial Payments Services

Evolution of Banking

- How did we get here?
- Current Payment Landscape

Bank Robbery Clip

Bank Robbery.mp4

Survey Says…

- 75% of surveyed organizations were victims of payments fraud in 2016
- 74% were exposed to business email compromise (BEC)
- Checks are the payment method most often exposed to fraud
- Wire transfers are the 2nd most-often targeted payment method

Source: 2017 AFP Payments Fraud and Control Survey

Payments Fraud & Fraud Prevention Tools

Check Fraud

75% of organizations experienced check fraud in 2016

For 25% of organizations that experienced fraud in 2016, the financial loss was less than $25,000.

32% of organizations suffered a financial loss between $25,000 and $249,000.

19% percent of organizations experienced a potential financial loss of at least $250,000.

According to the American Banker's Association, banks' **check fraud prevention systems were credited with keeping actual losses significantly lower** than the attempted fraud numbers.

Preventing Check Fraud

Positive Pay allows you to monitor paper checks presented for payment and reject unauthorized transactions before losses occur.

How it works
You simply submit an electronic file detailing the checks your business issues.

When items are presented for payment, a matching and validation process quickly identifies checks that don't match the data provided.

Images of exception items are provided online to provide your "pay" or "no pay" decisions.

Additional Benefits
Positive Pay not only helps prevent losses associated with paper check altering and counterfeiting, it also automates your account reconciliation process.

Wire Fraud

In 2016, wire transfers were the second most-often targeted payment method attacked by fraudsters.

46% of businesses with attempted or actual payments fraud reported that such attacks were via wire transfers.

2,370% increase in identified exposed losses from BEC between January 2015 and December 2016.

- Reported in all 50 states
- $346MM exposed losses in U.S. from June 2016 - December 2016

Source: FBI Public Service Announcement - Alert Number I-050417-PSA

Preventing Wire Fraud

"The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone.
Don't rely on e-mail alone." - Martin Licciardo, special agent, FBI Washington Field Office

- Call to verify the wire transfer request
- Train employees to identify these scams
- Verify any changes in vendor payment instructions
- Be suspicious of requests for secrecy or pressure to take action quickly
- Register all Internet domains that are slightly different than the actual company domain

ACH Fraud

In 2016, 30% of organizations were subject to ACH debit fraud and 11% to ACH credit fraud.

Primary sources of ACH fraud:

- ACH filters and/or blocks not utilized
- Gaps in online security controls

Preventing ACH Fraud

ACH Positive Pay allows your company to review incoming ACH transactions prior to posting. You can make a pay/return decision on rejected items.

ACH Filter allows only authorized debits to post to your account.

ACH Block allows you to block all ACH debits and/or credits.

Card Fraud – Data Security

2016 Cost of Data Breach Study

$221
the average cost of each lost or stolen record containing sensitive data

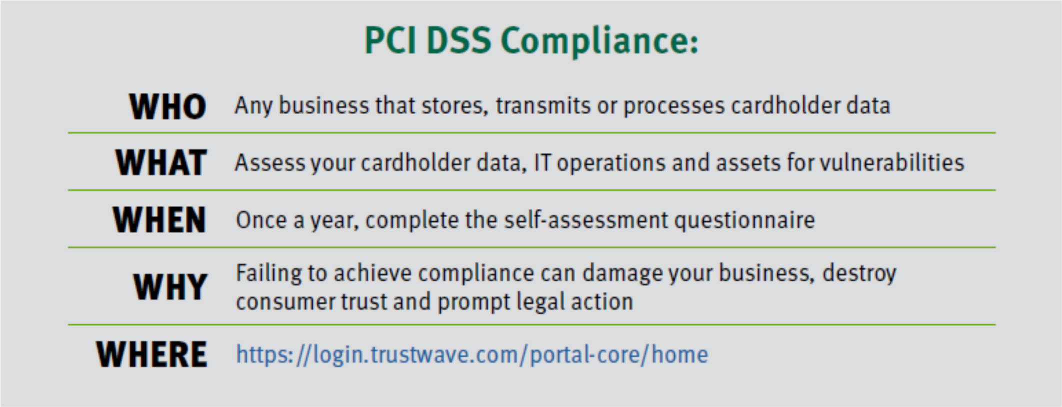
27%
of incidents include both IT and business process failures

7/10
of all attacks target small businesses

60%
of breaches target payment card data

Preventing Card Fraud

Consult with your credit card processor to ensure your business is **PCI compliant!**



PCI DSS Compliance:

WHO	Any business that stores, transmits or processes cardholder data
WHAT	Assess your cardholder data, IT operations and assets for vulnerabilities
WHEN	Once a year, complete the self-assessment questionnaire
WHY	Failing to achieve compliance can damage your business, destroy consumer trust and prompt legal action
WHERE	https://login.trustwave.com/portal-core/home

Best Practices

Best Practices

Verify Transactions

- Always carefully and thoroughly verify transactions for authenticity and promptly reconcile accounts.

- If you receive a request from a vendor to change routing information for an ACH or wire payment, you should authenticate the request to ensure it is legitimate by performing a call-back to a number you already have on file, as caller IDs and email addresses can be spoofed.

- Utilize same-day reporting to verify activity as quickly as possible during the banking day.

- If you believe any transactions are in error or were unauthorized, contact your bank immediately.

Best Practices

Separation of Duties

Commerce recommends a separation of duties between the individual verifying activity/reconciling accounts and the staff person(s) with authority to originate transactions.

The verifier/reconciler should not be given system authority to originate transactions.

Best Practices

Dual Controls

Commerce recommends that dual control approvals are completed from separate computers. Known malware is designed to capture multiple users' credentials on the same computer.

Commerce also requires initiation of ACH and wire payments under dual control: one person authorizes creation of the ACH or wire payment and a second person authorizes the release of the payment.

Best Practices

Mobile Devices

Mobile devices are becoming more frequent targets of cyber criminals. The following are best practices when conducting financial transactions from a mobile device.

- **Never** access bank accounts from cafés or public Wi-Fi hotspots
- Do not circumvent security features or otherwise "jailbreak" your mobile device
- Ensure encryption is turned on for your mobile device.
- Mobile devices should be password protected and auto lockout should be enabled
- Only download applications from trusted app stores

Combating Cyber Crimes

Tom C. Vincent II, GableGotwals

This presentation constitutes legal education and not legal advice. An attorney-client relationship is not created by this presentation. You should consult an attorney before taking any action that has legal consequences.

Combating Cyber Crimes – Tactics Used

- Phishing – using a fraudulent request or website to defraud someone
- Spearphishing – a type of phishing that uses particular information about the individual target (e.g. from social media)
- Spoofing – sending an e-mail that appears to be from one site but is actually from another (often used to divert contractor payments)
- Hacked e-mails from legitimate addresses (e.g. "clients" asking for their money)
- Loss or theft due to inside actors (e.g. employees)
- Ransomware – a malicious program that encrypts files on a system and may publish or delete the files
- Other attacks to influence stock prices (e.g. false tender offers)
- Theft of physical devices and storage media

NOT ALL REQUIRE "HACKS" – JUST HELP!

Combating Cyber Crimes – Structural Protection

- **Maintain Appropriate Rights/Responsibilities**
  - May involve additions and subtractions as responsibilities change
    - Hard vs. Soft Access, E-mail Groups/Committee Lists
  - Watch Lateral Hires
  - Communicate to Employee In Advance
  - Coordinate with IT
- **Provide Regular Training – Even Informally**
  - Specific regulations/requirements based on job function
    - Limit ability to act unilaterally, with additional limits as necessary (e.g. on transaction size)
  - Company policies/Contractual commitments
  - Sound day-to-day practices: computer, mobile device, email or other IT uses
    - e.g. What to send and how to send it – whether it's money or data
  - Incident Response – Not Just For Data Breaches
  - Reminder – "When in doubt, is your job worth it?"
- **Regular Testing and Verification Helps to Reinforce**
  - Social Engineering/Fraudulent emails
  - Performance Reviews

Combating Cyber Crimes – Day to Day

Personal Practices - Can Implement or Undermine Other Efforts

- Practice and reinforce basic IT protections
  - Choose strong passwords and secure them (don't share passwords or place on desks)
  - Shut down computers at least once a week to ensure any automatic updates are applied
  - Don't click random links online/in emails, from unknown individuals, with strange subject lines, or containing errors
  - Don't download software from the internet without review
  - Turn off WiFi unless needed to avoid automatically connecting
  - Pre-scan external hard drives/thumb drives and wipe when no longer needed
- Do not send out company information and/or funds without confirming the source *and reason* for the request – **a good source doesn't always mean a good reason!**
- Do not accept changes to normal processes at face value – confirm with a supervisor
  - Watch for unavailability re: call backs – "funeral," "bad cell service"
  - Ask first, then act later if appropriate

Combating Cyber Crimes – On the Way Out

- **Reminder of Data Security Responsibilities**
  - Personal Information vs. Company Information
  - Requirement to Return/Leave Proprietary Information
  - Consider Certification

- **Appropriate Timing for Access Limits/Termination**
  - Voluntary – Consider Appropriate Limitations on Access
  - Involuntary – Coordinate Notification with IT
  - Have a Plan for dealing with Personal Information
    - Requests should be centrally reviewed and addressed
  - Inventory Company Assets and Confirm Return

- **Exit Interview/Post Hoc Review**

Presenters

Commerce Bank

Carol Owens

SVP, Commercial Lending

Phone: (918) 477-3623
Carol.Owens@commercebank.com

Mellonie Lawlis

SVP, Treasury Services Manager

Phone: (918) 477-3620
Mellonie.Lawlis@commercebank.com

Matt Rodgers

Treasury Services Sales Officer

Phone: (918) 477-3603
Matt.Rodgers@commercebank.com

GableGotwals

Tom C. Vincent II, CRCM, CIPP/US

GableGotwals

Phone: (918) 595-4857
tvincent@gablelaw.com

Tom C. Vincent II brings extensive experience in regulatory compliance to his practice at GableGotwals. His background includes serving as chief compliance officer for different financial institutions, responsible for ensuring compliance with a myriad of requirements including customer protection, privacy, information security, and corporate governance.

Tom provides assistance to his clients with issues involving data security and privacy, including the establishment of cybersecurity programs, negotiation of appropriate protections for client information, breach identification and required reporting. Additionally, Tom has experience in investment advisory and trust and fiduciary compliance, and has held various broker-dealer and investment advisory securities licenses.