Fraud Update: *What We All Should Understand*

April 27, 2016

Charlene H. Craig
Senior Vice President
Not-For-Profit & Government Banking
404.230.1914
charlene.h.craig@suntrust.com

E. Douglas Hickman
Group Vice President
Foundations & Endowments Specialty Practice
404.588.7398
doug.hickman@suntrust.com

LaShonda Price
Vice President
Treasury & Payment Solutions
404.724.3301
lashonda.price@suntrust.com

Kathryn Vest
Senior Vice President
Private Wealth Management – Risk & Compliance
804.782.5606
kathryn.vest@suntrust.com

SunTrust

Agenda

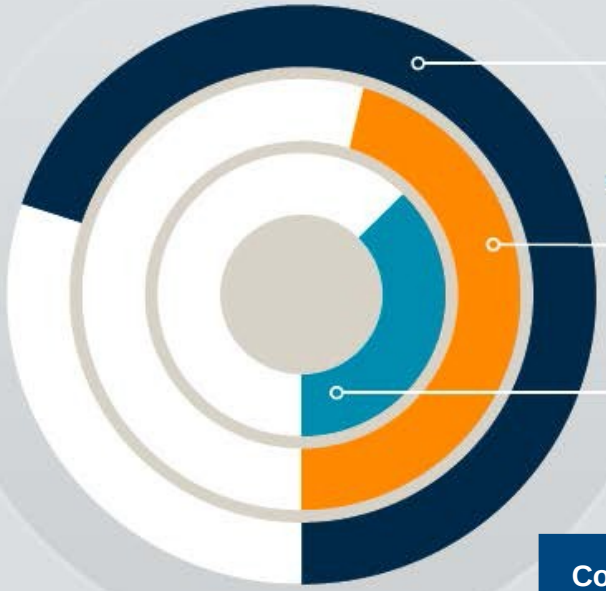
- Payment Fraud Trends
- Check Fraud
- ACH Fraud
- Card Fraud
- Wealth Management Fraud
- Social Engineering
- Ransomware
- Business Email Compromise
- Prevention Best Practices

2015 AFP Payments Fraud and Control Survey

62%

of companies were targets of payments fraud in 2014.

MOST TARGETED METHODS



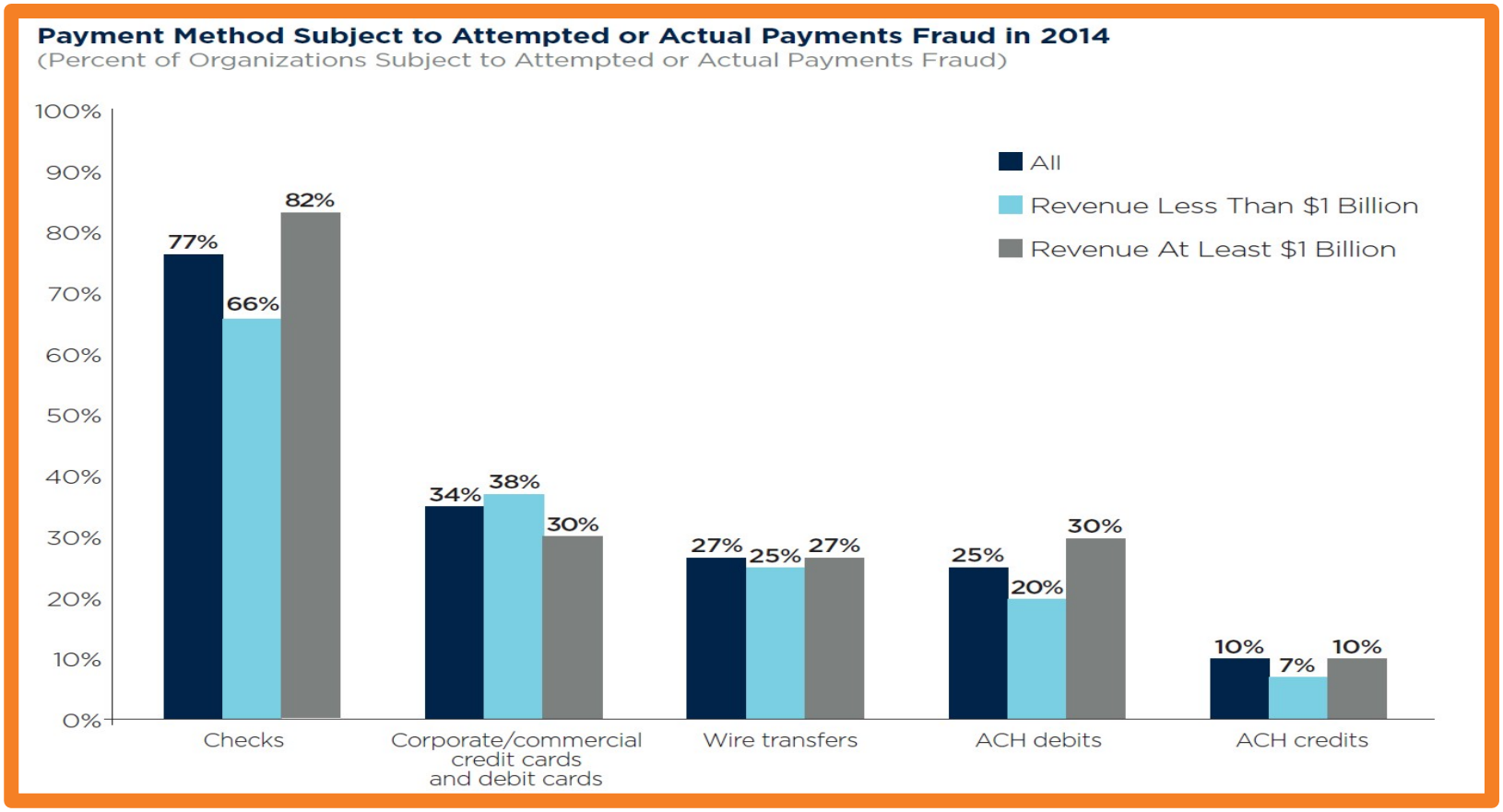
checks **77%**

credit/debit cards **34%**

wires **27%**

SunTrust

Payment Fraud Trends



SOURCE: 2015 AFP Payments Fraud and Control Survey

SunTrust

Check Fraud

- Counterfeit / Correct MCIR
- Altered Payee
- Altered Amount
- Fraudulent Account
- Loss / Theft of Check Stock
- Check Washing

Procedures Used to Prevent Check Fraud*	
Positive Pay	79%
Daily Reconciliation	73%
Segregation of Accounts	66%
Payee Positive Pay	44%
"Post No Checks" on Depository	39%
Reverse Positive Pay and Other	23%

**Percentages above are not intended to add up to 100%*

SOURCE: 2015 AFP Payments Fraud and Control Survey

SunTrust

ACH Fraud

- 73% of companies have had an attempt of ACH fraud*
- 11% of companies that have been exposed to ACH fraud experience financial loss*
- Of companies with more than 100 accounts, 26% suffer a financial loss due to ACH fraud*

Procedures Used to Prevent ACH Fraud *	
Reconcile Daily and Returns	75%
Block All ACH Debits – Except for a Dedicated ACH Account with Positive Pay/Filters	56%
Block ACH Debits on All Accounts	38%
Separate Account for Debits from Third Parties (e.g., Taxes)	31%
Debit Block Consumer Items with Debit Filter on Commercial Accounts	27%
Other	4%

**Percentages above are not intended to add up to 100%*

SOURCE: 2015 AFP Payments Fraud and Control Survey

Card Fraud

- Credit and debit cards experienced a decline in fraudulent activity, down from 43% in 2013 to 34% in 2014
- Card monetary losses are spread between organization, issuers, merchants, and processors

Reasons for Financial Loss from Corporate/Commercial Cards*	
Fraudulent Card Charges Made by a Third Party	54%
Lack of Internal Controls	18%
Employee Theft	15%
No Segregation of Duties	3%
Other	10%

**Percentages above are not intended to add up to 100%*

SOURCE: 2015 AFP Payments Fraud and Control Survey

SunTrust

Wealth Management Fraud

- Direct versus indirect access to wealth management accounts present different risks.
- Breaches of internal client email systems produce realistic looking requests.
- Copycat email addresses
- Wire transfer callbacks & segregation of duties
- Elder abuse

SunTrust

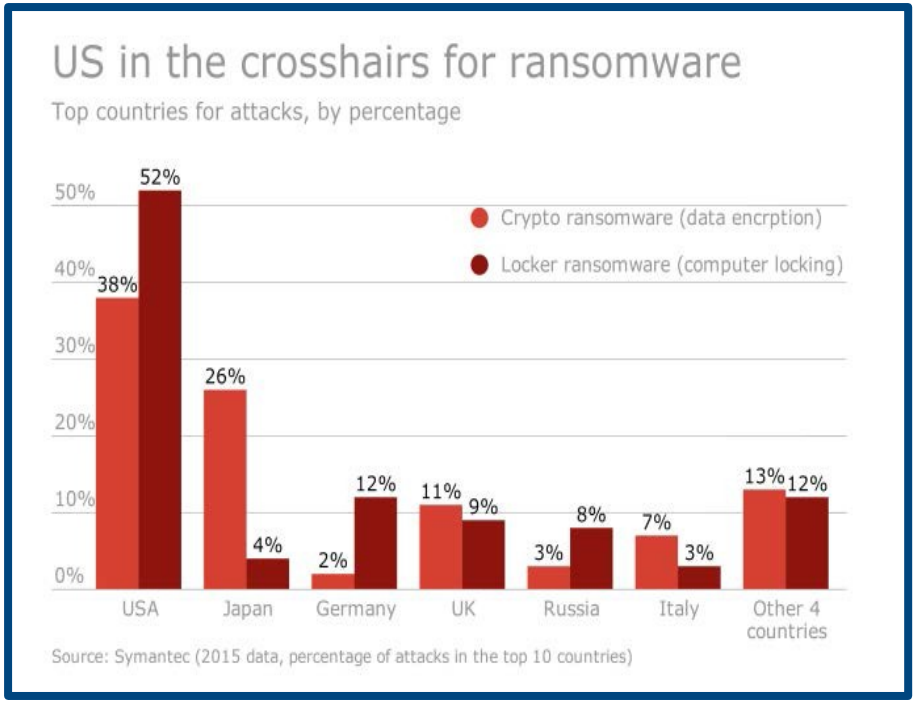
Social Engineering

- Phishing (Email)
- Smishing (Text Message)
- Vishing (Voicemail)
- Twishing (Twitter)
- Search Engine Poisoning
- Malware: Trojans, Viruses
- Trusted Site Compromise
- Fake Mobile Apps

Avoid Getting Hooked By a Phish…

SunTrust

Ransomware



Hollywood Presbyterian 2/16
$17K in Bitcoin ransom paid

Ransomware Types:
Locker – Disables access & control
Crypto - Encrypts data

- In 2015 there were nearly 2,400 reported ransomware incidents
- Victims paid more than $24 million encryption keys to unlock phones, computer files and entire computer systems following the installation of this malware

SunTrust

Ransomware

The FBI offers the following tips to protect devices from ransomware:

- Ensure you have updated antivirus software on your devices
- Enable automated patches for your operating system and web browser
- Use strong passwords unique to each account
- Use a pop-up blocker
- Download software, games, and programs (especially those that are free) only from sites known and trusted sites
- Don't open attachments in unsolicited e-mails and never click on a URL contained in an unsolicited e-mail. Close out the e-mail and go directly to the organization's website.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.
- Conduct regular system back-ups and store the backed-up data offline.

Business Email Compromise

- **Business Executive Fraud** - Email accounts of high-level business executives (CFO, CTO, etc.) are mimicked or hacked, and a transfer request is made to someone who processes wires
- **Bogus Supplier Invoices** - A business, often with a long-standing supplier relationship, is asked to wire funds to pay an invoice to an alternative, fraudulent account via email
- **Purchase Order** - An employee's email account is hacked, recent email is reviewed, and fraudulent invoice requests are sent to vendors

SunTrust

Business Email Compromise - Invoice

Spoofed or Hacked Supplier Email

Legitimate User: Accounts Payable Team

Change Invoice and Payment Instructions

Criminal Beneficiary receives funds

Criminals learn about their targets from online sources. They leverage company websites, press releases, and company directories.

They monitor emails, to determine normal process flow and optimal timing. They "sound " like a legitimate vendor. New supplier lookalike domains can be created.

They control email flows and create new email rules to avoid detection. Fake conversations about the invoice can take place without the associate realizing the breach.

BEC Amounts are generally in a range of normal invoice activity.

SunTrust

Business Email Compromise Mitigation Best Practices - Invoice

- Know Your Vendor - Verify Your New Vendor is a Legitimate Organization
  - Perform due diligence on the company's background and existence
  - Dual approvals for new vendors
  - Email requests for new vendor set-up not accepted
- Plan How Your Vendor Will Connect to You
  - EDI, secure FTP, Web portal, Phone
  - Test, document, and validate
- Segregate Responsibility of Vendor Authentication and Purchasing Functions
- Changes to Vendor Master File : Requests must be validated by trusted source at vendor
- Verbal Confirmation – Vendors should be required to verbally approve changes using phone numbers that are known and listed for vendors
- Vendor list, including contact information of individuals authorized to make payment changes, should be kept in a hard copy file
- Train associates on all vendor management policies and empower them to ask questions when in doubt.
- New Vendor system flags

Business Email Compromise – Wire Transfer

Spoofed or Hacked CEO Email

Criminals learn about their targets from online sources. They leverage company websites, press releases, and company directories.
They monitor emails, and create a sense of urgency and importance around the fraudulent request.

Legitimate User: CFO, Controller

They "sound " like the legitimate source. Spoofed emails very closely mimic a legitimate emails Requests are well-worded and specific to the business victims.
Requests coincide with business travel dates for executives whose emails were spoofed.

Wire Transfer Sent

BEC Amounts are generally in a range of normal client wire transfer activity to avoid suspicion or detection.

Criminal Beneficiary receives funds

BEC Beneficiary banks are both domestic and international

SunTrust

Business Email Compromise Mitigation Best Practices – Wire Transfer

- Educate your staff about the fraud risks inherent in their daily processes.
- Create a culture that empowers employees to ask questions especially when there is a request for secrecy, to bypass normal operating procedures or pressure to take action quickly.
- Develop processes for wire validation that include access to key executives for approval.
- Require two people to approve the movement of large sums or to make changes to any information that impacts the movement of funds.
- Verify important or large transactions through an alternate method including phone call or in-person.
- Establish a company website domain and use it to create company email accounts. Do not use free, web-based email accounts for business purposes.
- Limit the amount of information available to the general public about your company's internal operations.
- Conduct all banking on a dedicated machine used for no other task. Create dedicated virtual operating system for the sole purpose of providing a secure environment.

Password Security

Don’ts

- Never use the “remember password” feature
- Never use your name, phone number, a number series (e.g., “123456”), or an easily-guessed word (e.g., “password”)
- Never share your password
- Never write down your password

Do’s

- Use a different password for each account
- Change your password often
- Use a combination of upper/lower case, numbers, and special characters
- Use long passwords

- Substitute numbers for letters and vice versa
- Use capitalization in random places, intentionally misspell words, or spell them backwards
- Use words then remove letters and add relevant numbers: First Car — 1992 Ford Mustang = FdMstg92
- Use phrases substituting letters with numbers: The party is at 7 o'clock = prtyzat7
- Experiment with your favorite song, album, or movie titles by adding numbers: Michael Jackson’s Thriller = MJAXtHri13r

Avoiding Security Breaches - Best Practices

Multiple Layers of Security are Critical:

- Train employees
- Empower employees
- Develop and communicate clear cyber-security policies
- Have off site data back-up and data loss prevention technologies
- Use strong passwords and change often
- Keep up-to-date anti-virus and anti-spyware software
- Leverage layered security methods (e.g. Trusteer Rapport)*
- Use dedicated machines for financial transactions
- Safeguard facilities and devices
- Don't trust email

*Trusteer Rapport is a secure browsing software provided by SunTrust for certain online applications that are used by SunTrust clients. The software, which is downloaded to, or accessed by, your computer or mobile device, is provided by Trusteer, an IBM Company, Boston, MA.

THANK YOU

SunTrust