AFP® Annual Conference

Association for Financial Professionals®

OCTOBER 27–30, 2013 | LAS VEGAS

ORIGINAL→ESSENTIAL→UNBIASED→INFORMATION

Best Practices in Treasury Security

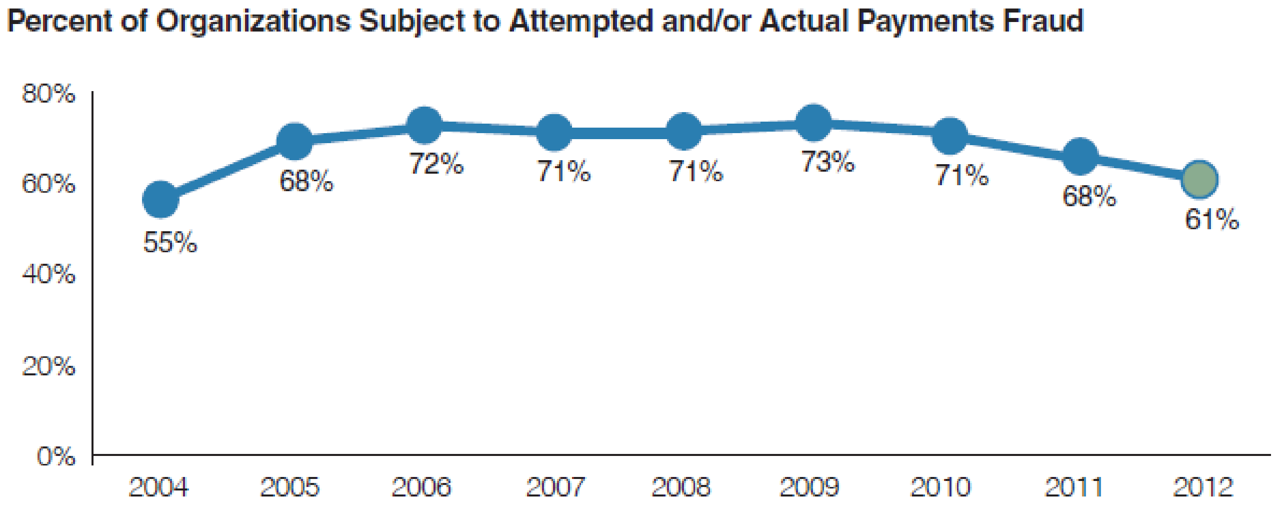
Mark Griffin
MLGriffin@BBandT.com

Jon Rier
jrier@racetrac.com

Jose Paniagua
jpaniagua@arbys.com

Why treasury security matters

61% of AFP Payments Fraud and Control Survey respondents experienced actual or attempted payments fraud in 2012!



- The good news: Nearly 3/4 of these organizations also reported no financial losses due to the attempted fraud
- The main reason for low actual losses = <u>effective fraud detection and controls!</u>

Source: 2013 AFP Payments Fraud and Control Survey

Objective: To share best practices involving treasury security and controls; discuss methods to prepare for fraud attempts

Agenda:

- General best practices
- Internal fraud
- Payment type specific fraud
  - **Various payment types (check, ACH debit, corporate card)**
  - **Account takeovers (malware, phishing, man-in-the-middle, DDoS)**
- Recent regulatory actions
- Retail fraud
  - **Cash handling**
  - **Credit/debit card fraud prevention**
- Research and other resources on treasury security

General Best Practices

Implementing these general best practices is the <u>best and easiest way</u> to prevent losses from internal and external fraud!

- Reconcile bank accounts daily
  - Detect errors or suspicious activity quickly
  - Minimize size/scope of any fraud
  - May be able to reverse/return fraudulent items
  - Nearly 75% of AFP Fraud survey respondents reconcile daily*
- Segregation of duties
  - Different people or groups responsible to initiate, approve, and reconcile treasury activity
  - Reduces risk of internal fraud by requiring more than one party be involved
  - More eyes on activity to catch suspicious activity/errors

*Source: 2013 AFP Payments Fraud and Control Survey

General Best Practices (cont.)

- Dual administrators/payment approval
  - Requires more than one party to approve payments or change user entitlements
  - External account takeover is more difficult – requires two users information be compromised
  - To streamline workflow – set up approved templates for recurring payments
- Set meaningful limits
  - Can set limit by wire/ach template, by user, by day, internally, etc.
  - Set limits that will alert you to odd activity
    - Avoid meaningless limits that are too high or too low
- Document and audit your controls
  - Identify controls and audit to ensure they are in place
  - Never document/share any user specific information!

Internal Fraud Threats

- Internal fraud and errors are typically the **largest contributor** to overall losses!
- General best practices = most effective prevention
- Internal sources are most familiar with security procedures
    - Most likely to know how to avoid them
- Think like a fraudster! As a treasury professional it's your job to question everything and not rely on trust (though trust is important!)
- Other items to consider:
    - Background or credit checks
    - Avoid "super users" – the only person who has knowledge of certain payment processes
        - If limited resources dictate super users – ensure regular audits/oversight
    - Forensic accounting audit of procure to pay process

Check Fraud

In 2012, **87%** of all reported payment fraud attempts were **check fraud**!

Measures to prevent check fraud:

- Positive pay
- Payee match
- Large dollar item exceptions
  - Every check over $___ is identified as an exception
  - Even if all else matches…one last set of eyes
- Dual approval on exceptions
  - Otherwise the exception approver could choose to “pay” anything
- Is your positive pay file secure?
  - Is it encrypted? Can it be manually adjusted?
  - Who has access to the file?
  - Feedback from bank confirming the dollar totals and number of items?

Source: 2013 AFP Payments Fraud and Control Survey

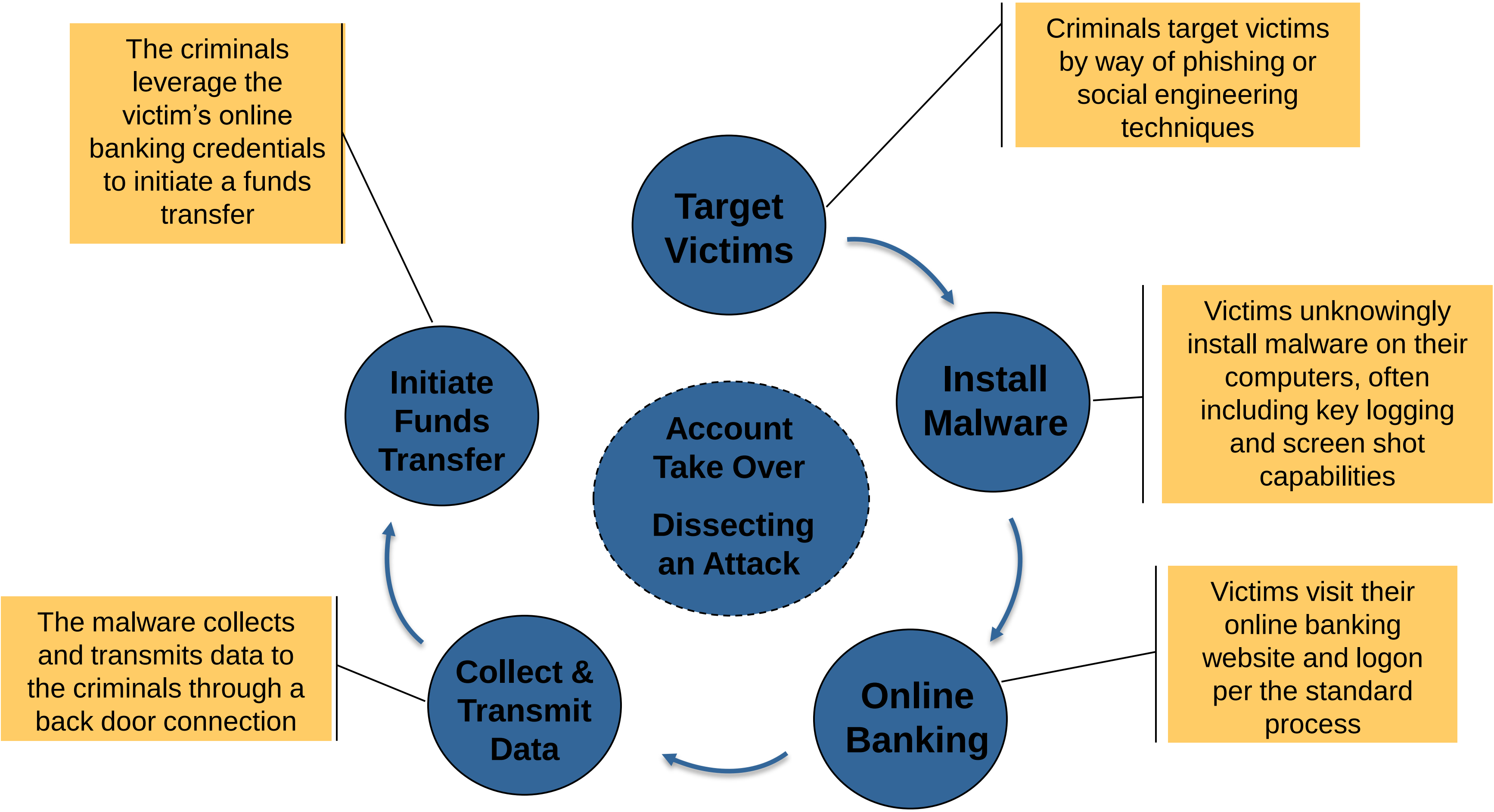
ACH/Wire Fraud

As the use of electronic payments continues to rise, so will the prevalence of electronic payment fraud attempts.

Measures to prevent ACH/wire fraud:

- General best practices
  - Dual authentication/approval, appropriate limits by user/account/template/day, daily reconciliation, etc.
- ACH Blocks
  - If the account does not need ACH capability, block all incoming debits!
  - Relatively cheap way to ensure no fraudulent debits
- ACH Filters or ACH "Positive Pay"
  - Allows only authorized debits to the account
  - Be careful – still require dual approval as in check positive pay
- Use bank's online system, Treasury workstation or ERP system to initiate – not fax/phone
- Email alerts for processed ACH/wire activity

Account Takeover Attacks



Criminals target victims by way of phishing or social engineering techniques

Victims unknowingly install malware on their computers, often including key logging and screen shot capabilities

Victims visit their online banking website and logon per the standard process

The malware collects and transmits data to the criminals through a back door connection

The criminals leverage the victim's online banking credentials to initiate a funds transfer

Source: Joint Fraud Advisory for Businesses: Corporate Account Take Over by USSS, FBI, IC3 and FS-ISAC.

Common methods for account takeover

Criminals are constantly evolving new ways to steal and use your information:

- Phishing/Whaling
  - Correspondence that appears to be from your bank – designed to trick you into providing your bank credentials
  - Executives more at risk (whaling)
  - If admin information is compromised, may circumvent all security controls
- Malware/Spyware/Key-loggers
  - Links, attachments, websites, downloads, emails – can all contain malicious software
  - Captures sensitive information to be used in account takeover
- Man-in-the-middle/Man-in-the-browser
  - Fraudster directs you to a mirror image of your bank website
  - Intercepts authentication information and uses it to create fraudulent transactions
  - Affected browser – fraudster alters actual transactions through actual approval channels

Preventing account takeover

Again, general best practices are your first line of defense. In addition:

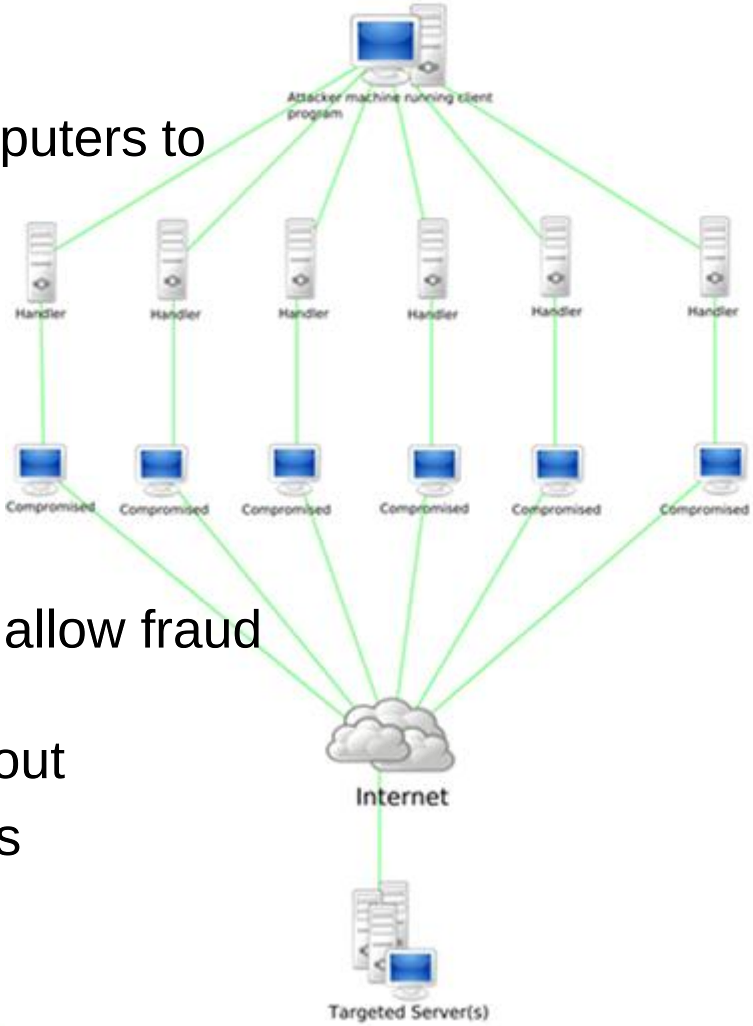
- Educate users
  - Don't click on unknown items, links, etc.; don't provide any user specific information unless to a known bank representative
  - People will make mistakes – don't rely on education alone!
- Token passwords
  - Require for both access and initiating payment
  - Limits usefulness of any stolen credential information

- Trusteer Rapport or other similar products
  - Identify trusted bank websites
  - Warn users against behavior that may potentially give away credentials
- Segregated workstations
  - Treasury activity done from system that has limited/locked access
  - Limits opportunities for credentials to be compromised
  - Make sure users are educated to only use these workstations
- Out-of-band verification for certain payment types (wires, etc.)

Is DDoS a risk to corporate treasury?

DDoS = distributed denial of service

- Hackers use a network of affected computers to overload servers and prevent activity
- Targeted banks, with little success
- Corporates have not typically been targets BUT – DDoS may be used as a distraction to overwhelm defenses and allow fraud
- Talk to your bank and your IT group about DDoS as part of disaster recovery plans
- Potential retail issues?



Who is responsible for losses from account takeovers?

Who takes the loss, the customer or the bank?

Based on the responses to the most recent AFP Fraud survey, it appears the answer is not fully understood!

- Check your Treasury Agreements
  - Both parties are typically required to maintain “reasonable commercial standards”
  - Interpretation of these standards has led to several lawsuits between bank and customer
  - Bottom line for customer: if the bank offers the security, likely in your best interest to use it
  - Banks have also been penalized for not keeping technology current – so talk to your bank about their investment in security measures

What else are banks doing to add security?

Transaction monitoring is deployed to monitor client behavior:

- Transactions history
- Amounts
- Destination of transaction
- New payee
- Hot spots – known fraud elements (payee, location, etc.)

Alerts are created and the transactions are stopped for fraud review

Once alert is researched, clients may be called for verification

Transactions are released after verification

What has the government response been?

- Federal Financial Institutions Examinations Council (FFIEC)
- Issuing guidance “Authentication in an Internet Banking Environment”
- Banking guidance to address the rise in cyber crime
- Cyber crime complaints steadily rising, particularly with commercial accounts
- “Since virtually every authentication technique can be compromised, financial institutions should not rely on any single control for authorizing high-risk transactions, but rather institute a system of layered security.”

Retail fraud prevention

In addition to previously mentioned internal, external, and payment specific fraud risks, retail organizations also must work to minimize potential payment fraud at dispersed locations

General Best Practices:

- Document cash and credit card handling policies
  - Audit often – at least once a year
- Maintain communication with Field Operations leadership
  - Identify weaknesses that are being or could be exploited
  - Work with Operations and various vendors to shore up possible weaknesses ASAP
- Develop metrics to identify better/poor performing stores
  - Define standard performance (e.g., store over/short, deposit discrepancies, change order frequencies, timeliness, chargebacks, etc…)
  - Tailor certain incentives to performance vs. standard metrics

Smart Safes

When combined with general best practices, Smart Safes can be an excellent tool in the prevention of cash loss

- The commoditization of these products have made them more flexible and affordable
  - Still an expensive proposition for smaller retailers
- However, they provide the following benefits:
  - Safer environment for employees
  - Dollar validation and counterfeit detection
  - Immediate credit
  - Daily reporting - some vendors have intraday capabilities
  - Bank consolidation; reconciliation benefits
  - Labor reduction

- The more flexible and more expensive programs will be bank and armored carrier agnostic
- Bundled packages by market players can present significant savings

Credit Card Handling & PCI

Payment card fraud (credit card, debit card, etc.) is one of the biggest fraud issues facing any retailer. Here are some general card handling processes to help prevent loss:

- If possible, swipe card at the point of sale or register
  - Manual entry of card number as a last resort
  - If taking remote payment, additional security layer (ZIP-code prompting, security-code prompting) should be in place
  - PIN entry typically results in lowest fraud
  - Require signatures on receipts over certain dollar amount ($25)

- PIN-pads & card readers
  - Prefer consumer facing PIN-pad – reduces potential for internal fraud
  - If not feasible – employ process where employees only ask for the card when ready to swipe; ensure card is always visible, returned immediately
  - If possible, install secure card readers to reduce risk of skimming. Still need regular field checks to prevent skimming.

Credit Card Handling and PCI (cont.)

- Verify ID where feasible
  - If possible, ensure name on receipt matches name on card
  - Evaluate speed of service/inconvenience of other ID checks
- No Cash Refunds
  - Allow customer to dispute through bank or give a credit
  - Potential for customer dissatisfaction with time until credit is received
- EMV Policy
  - EMV liability shift will be effective October 1, 2015, (fuel-selling merchants will have an additional two years to become compliant)
  - Develop procedures to prepare for/prevent additional liability
- Other PCI considerations:
  - How often are scans executed against your card processing environment?
  - How often are hardware and software programs reviewed for obsolescence?
  - Do you prefer an Integrated POS and payments acceptance system or a separate terminal for payments?

Questions??

Appendix & Resources

Online Banking Fraud Resources

2013 AFP Payments Fraud and Control survey: http://www.afponline.org/fraud/

American Banker: How Banks can win the cyber war:

http://www.americanbanker.com/video/how-banks-can-win-the-cyber-war1057581-1.html

Recent articles concerning payments fraud disputes:

American Banker: Court Sides with Bank against wire transfer victim

http://www.americanbanker.com/issues/178_66/court-sides-with-bancorpsouth-against-wire-transfer-fraud-victim-1058073-1.html

Bank Watch: Bank sued by customer, alleged not providing reasonable security

http://obsbankwatch.blogspot.com/2013/04/bank-of-granite-facing-lawsuit-after.html

American Banker: Courts find bank’s anti-fraud tech inadequate

http://www.americanbanker.com/btn/25_8/federal-court-finds-ocean-bank-anti-fraud-tech-inadequate-1051180-1.html

DDoS information:

BankInfoSecurity.com: Lessons learned from Bank DDoS attacks

http://www.bankinfosecurity.com/lessons-learned-from-bank-ddos-attacks-a-6049

American Banker: Banks hit with new waive of DDoS attacks

http://www.americanbanker.com/issues/178_145/regions-bank-hit-with-new-ddos-attack-1060942-1.html