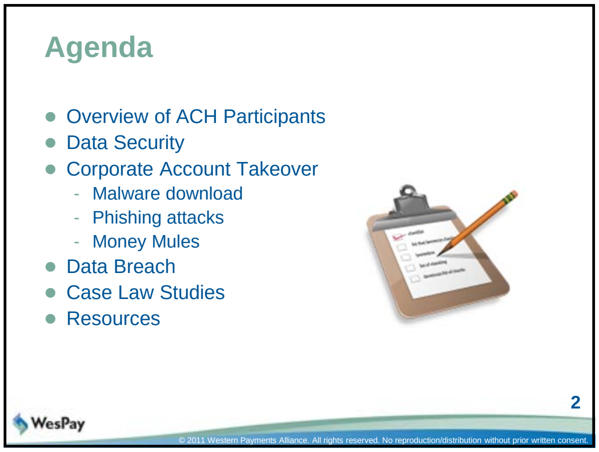
WesPay

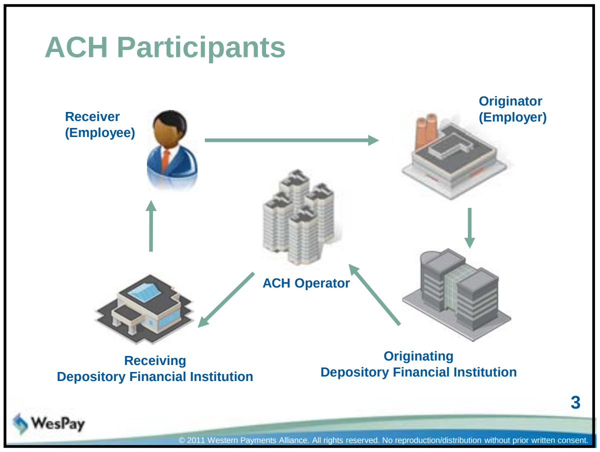
Protect Your Company from Cyber-theives

Patty Presta, AAP, VP of Education

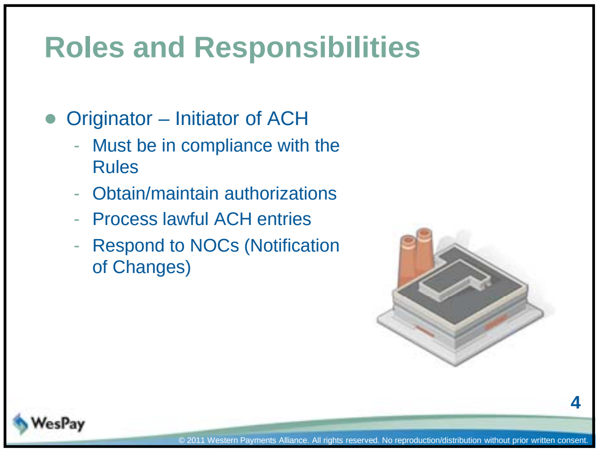


Agenda

- Overview of ACH Participants
- Data Security
- Corporate Account Takeover
  - Malware download
  - Phishing attacks
  - Money Mules
- Data Breach
- Case Law Studies
- Resources

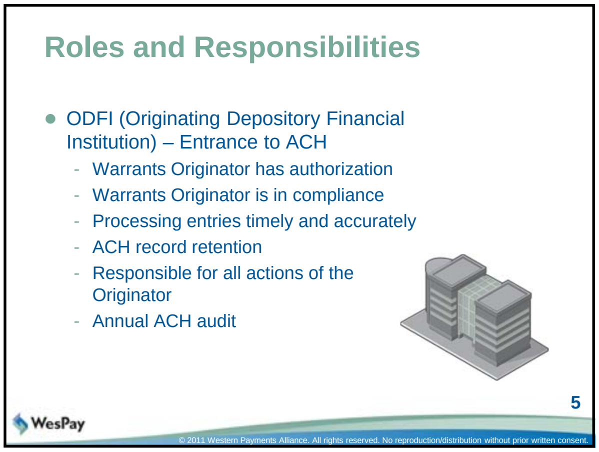


ACH Participants



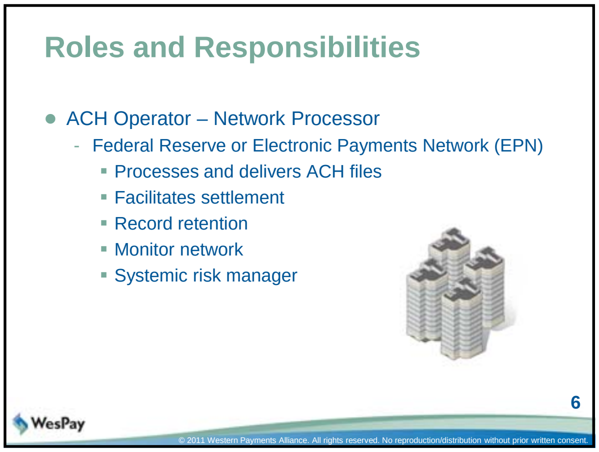
Roles and Responsibilities

- Originator – Initiator of ACH
  - Must be in compliance with the Rules
  - Obtain/maintain authorizations
  - Process lawful ACH entries
  - Respond to NOCs (Notification of Changes)



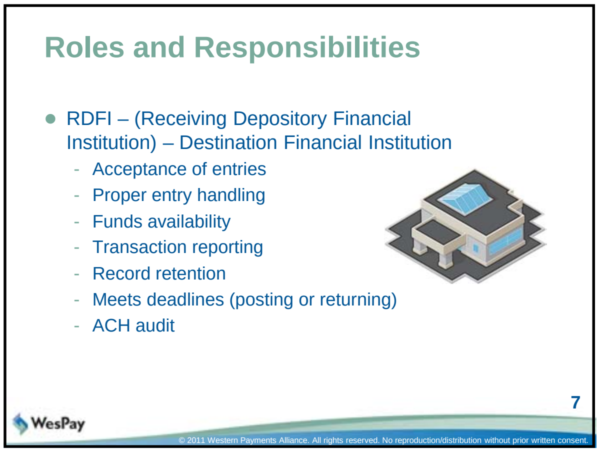
Roles and Responsibilities

- ODFI (Originating Depository Financial Institution) – Entrance to ACH
  - Warrants Originator has authorization
  - Warrants Originator is in compliance
  - Processing entries timely and accurately
  - ACH record retention
  - Responsible for all actions of the Originator
  - Annual ACH audit



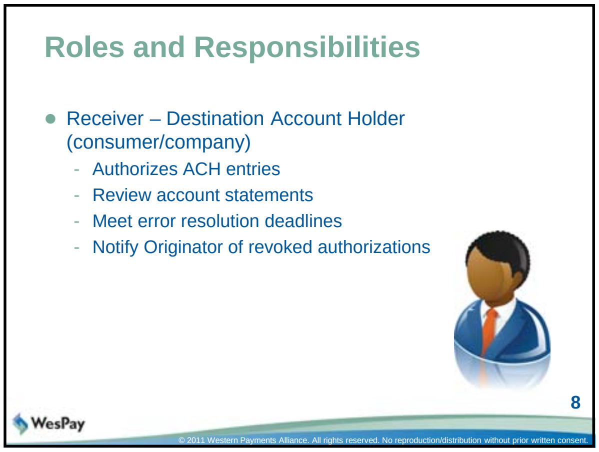
Roles and Responsibilities

- ACH Operator – Network Processor
  - Federal Reserve or Electronic Payments Network (EPN)
    - Processes and delivers ACH files
    - Facilitates settlement
    - Record retention
    - Monitor network
    - Systemic risk manager



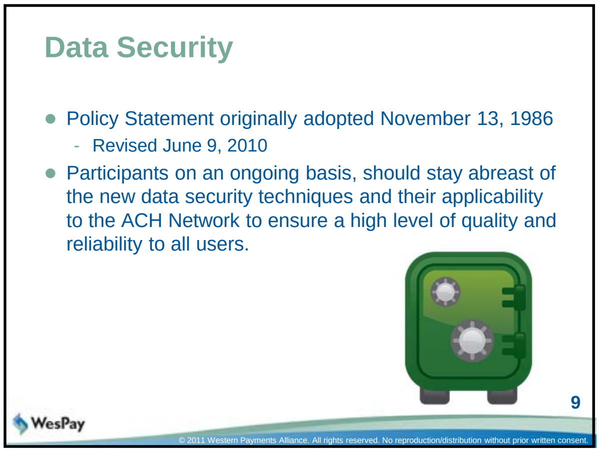
Roles and Responsibilities

- RDFI – (Receiving Depository Financial Institution) – Destination Financial Institution
  - Acceptance of entries
  - Proper entry handling
  - Funds availability
  - Transaction reporting
  - Record retention
  - Meets deadlines (posting or returning)
  - ACH audit



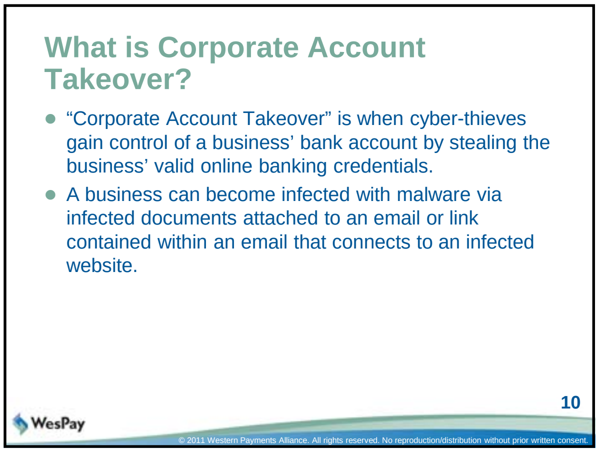
Roles and Responsibilities

- Receiver – Destination Account Holder (consumer/company)
  - Authorizes ACH entries
  - Review account statements
  - Meet error resolution deadlines
  - Notify Originator of revoked authorizations



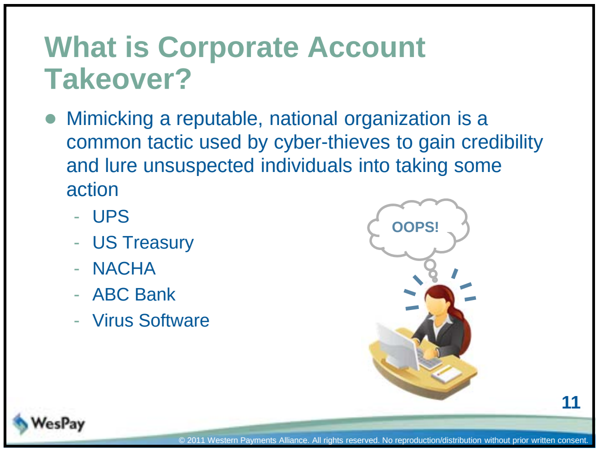
Data Security

- Policy Statement originally adopted November 13, 1986
  - Revised June 9, 2010
- Participants on an ongoing basis, should stay abreast of the new data security techniques and their applicability to the ACH Network to ensure a high level of quality and reliability to all users.



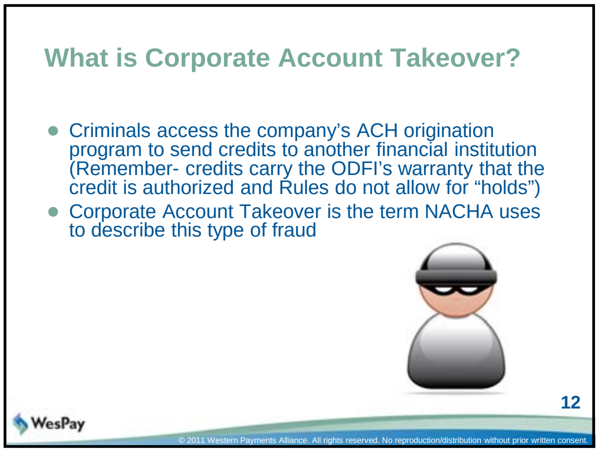
What is Corporate Account Takeover?

- “Corporate Account Takeover” is when cyber-thieves gain control of a business’ bank account by stealing the business’ valid online banking credentials.
- A business can become infected with malware via infected documents attached to an email or link contained within an email that connects to an infected website.



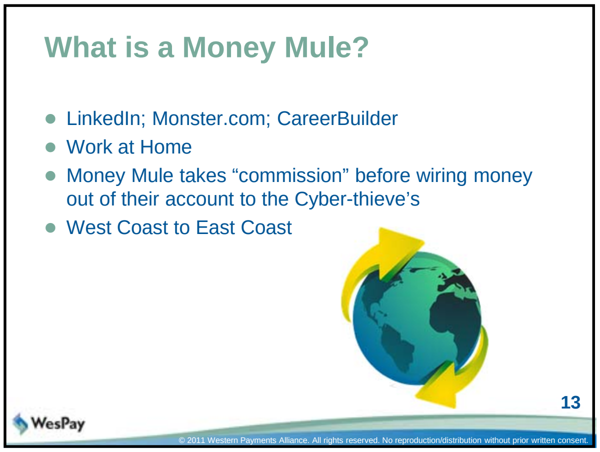
What is Corporate Account Takeover?

- Mimicking a reputable, national organization is a common tactic used by cyber-thieves to gain credibility and lure unsuspected individuals into taking some action
  - UPS
  - US Treasury
  - NACHA
  - ABC Bank
  - Virus Software



What is Corporate Account Takeover?

- Criminals access the company’s ACH origination program to send credits to another financial institution (Remember- credits carry the ODFI’s warranty that the credit is authorized and Rules do not allow for “holds”)
- Corporate Account Takeover is the term NACHA uses to describe this type of fraud

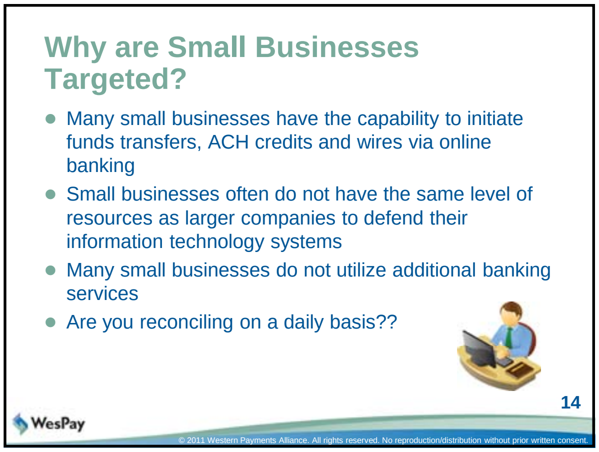


What is a Money Mule?

- LinkedIn; Monster.com; CareerBuilder
- Work at Home
- Money Mule takes “commission” before wiring money out of their account to the Cyber-thieve’s
- West Coast to East Coast

13

WesPay

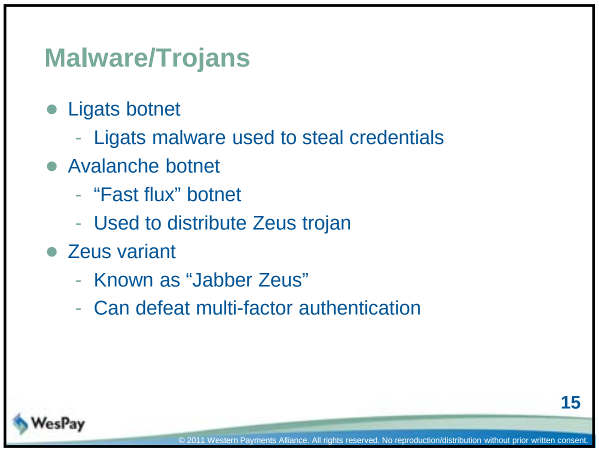


Why are Small Businesses Targeted?

- Many small businesses have the capability to initiate funds transfers, ACH credits and wires via online banking
- Small businesses often do not have the same level of resources as larger companies to defend their information technology systems
- Many small businesses do not utilize additional banking services
- Are you reconciling on a daily basis??

14

WesPay

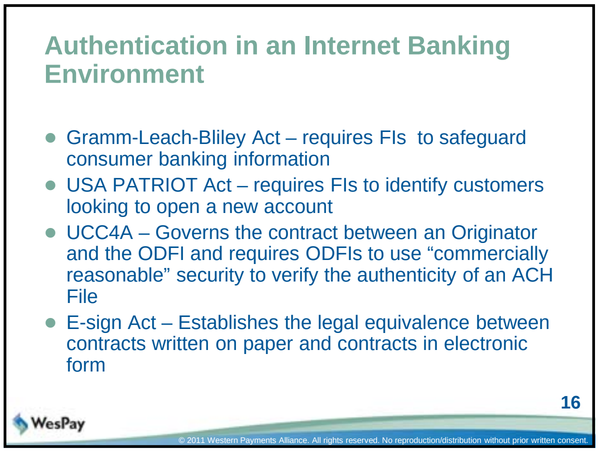


Malware/Trojans

- Ligats botnet
  - Ligats malware used to steal credentials
- Avalanche botnet
  - “Fast flux” botnet
  - Used to distribute Zeus trojan
- Zeus variant
  - Known as “Jabber Zeus”
  - Can defeat multi-factor authentication

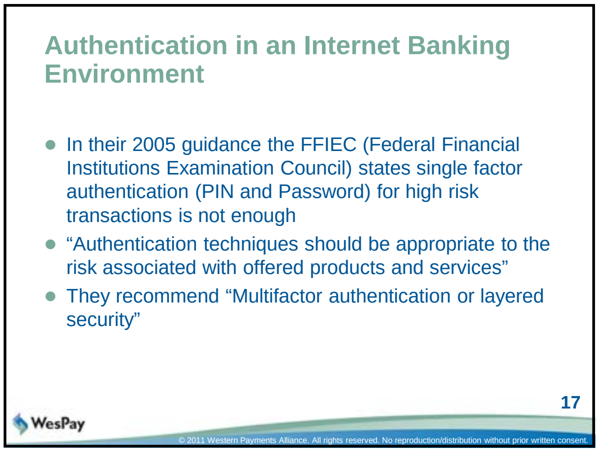
15

WesPay



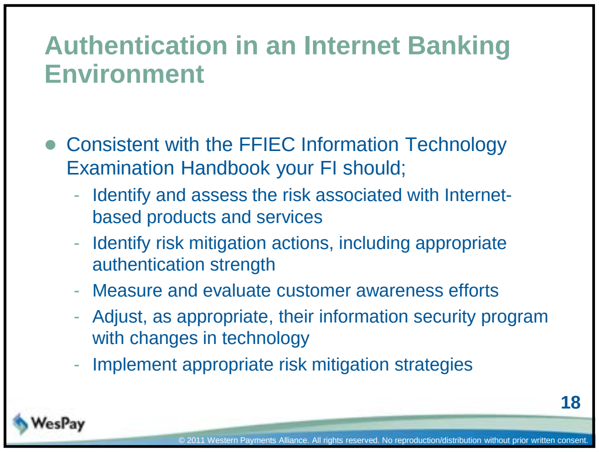
Authentication in an Internet Banking Environment

- Gramm-Leach-Bliley Act – requires FIs to safeguard consumer banking information
- USA PATRIOT Act – requires FIs to identify customers looking to open a new account
- UCC4A – Governs the contract between an Originator and the ODFI and requires ODFIs to use “commercially reasonable” security to verify the authenticity of an ACH File
- E-sign Act – Establishes the legal equivalence between contracts written on paper and contracts in electronic form



Authentication in an Internet Banking Environment

- In their 2005 guidance the FFIEC (Federal Financial Institutions Examination Council) states single factor authentication (PIN and Password) for high risk transactions is not enough
- “Authentication techniques should be appropriate to the risk associated with offered products and services”
- They recommend “Multifactor authentication or layered security”



Authentication in an Internet Banking Environment

- Consistent with the FFIEC Information Technology Examination Handbook your FI should;
  - Identify and assess the risk associated with Internet-based products and services
  - Identify risk mitigation actions, including appropriate authentication strength
  - Measure and evaluate customer awareness efforts
  - Adjust, as appropriate, their information security program with changes in technology
  - Implement appropriate risk mitigation strategies

Authentication in an Internet Banking Environment

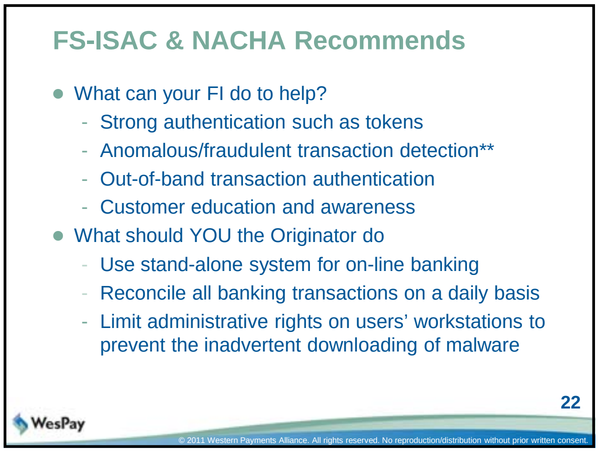
- Recommendations for authentication methodologies include;
  - Something the user knows (PIN and Password)
  - Something the user has (token ID or UBS device)
  - Something the user is (biometric characteristic)
  - Out of Band verification (Fax or call back)

Authentication in an Internet Banking Environment

- Device Identification
  - A cookie loaded onto the customers computer
    - Issue – cookies can be copied and pasted onto the fraudster's PC to replicate the point of origination. A more complex digital identification may resolve some of these issues by checking things like device configuration
  - Challenge Questions
    - Issue – key-logging software may enable the fraudster to capture the "answer" provided in previous sessions, and certain answers may be easily assessable via the internet. Out-of-wallet questions that do not rely on information that is easily assessable and multiple questions asked at random may alleviate some of these issues

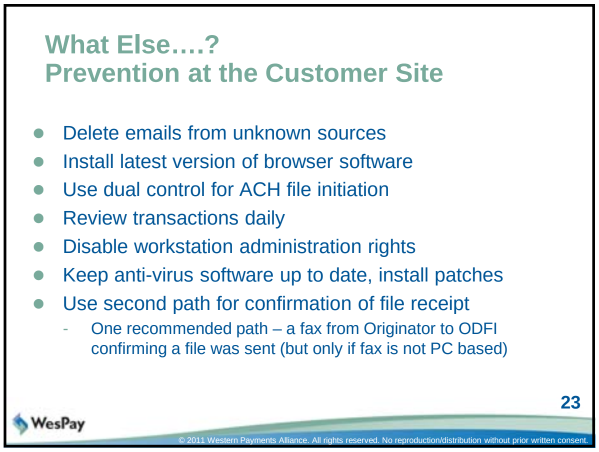
Authentication in an Internet Banking Environment

- Layered Security Programs may include (but are not limited to);
  - Fraud detection and monitoring systems
  - Dual customer authorization through different access devices
  - The use of out-of-band verification
  - The use of "positive pay" debit blocks and other techniques
  - Enhanced controls over account activities
  - IP reputation-based tools



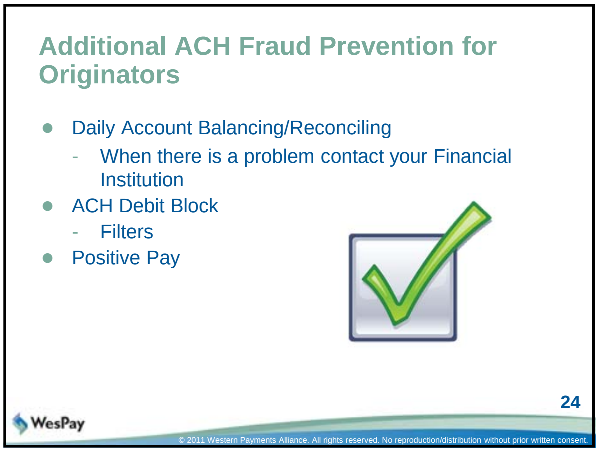
FS-ISAC & NACHA Recommends

- What can your FI do to help?
  - Strong authentication such as tokens
  - Anomalous/fraudulent transaction detection**
  - Out-of-band transaction authentication
  - Customer education and awareness
- What should YOU the Originator do
  - Use stand-alone system for on-line banking
  - Reconcile all banking transactions on a daily basis
  - Limit administrative rights on users' workstations to prevent the inadvertent downloading of malware



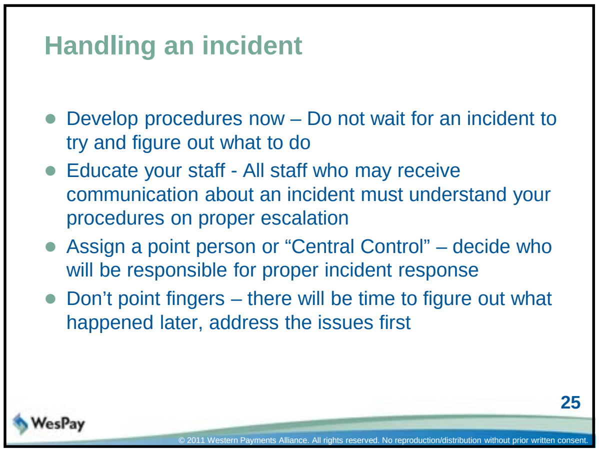
What Else….?
Prevention at the Customer Site

- Delete emails from unknown sources
- Install latest version of browser software
- Use dual control for ACH file initiation
- Review transactions daily
- Disable workstation administration rights
- Keep anti-virus software up to date, install patches
- Use second path for confirmation of file receipt
  - One recommended path – a fax from Originator to ODFI confirming a file was sent (but only if fax is not PC based)



Additional ACH Fraud Prevention for Originators

- Daily Account Balancing/Reconciling
  - When there is a problem contact your Financial Institution
- ACH Debit Block
  - Filters
- Positive Pay

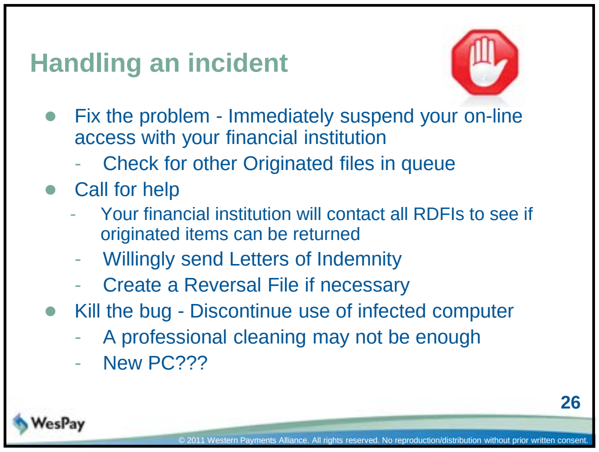


Handling an incident

- Develop procedures now – Do not wait for an incident to try and figure out what to do
- Educate your staff - All staff who may receive communication about an incident must understand your procedures on proper escalation
- Assign a point person or “Central Control” – decide who will be responsible for proper incident response
- Don’t point fingers – there will be time to figure out what happened later, address the issues first

25

WesPay

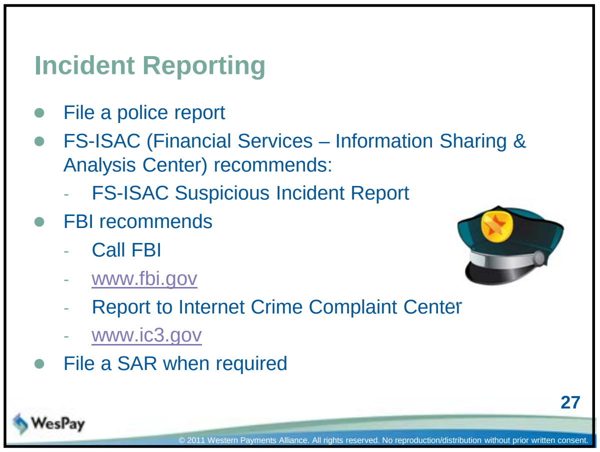


Handling an incident

- Fix the problem - Immediately suspend your on-line access with your financial institution
  - Check for other Originated files in queue
- Call for help
  - Your financial institution will contact all RDFIs to see if originated items can be returned
  - Willingly send Letters of Indemnity
  - Create a Reversal File if necessary
- Kill the bug - Discontinue use of infected computer
  - A professional cleaning may not be enough
  - New PC???

26

WesPay

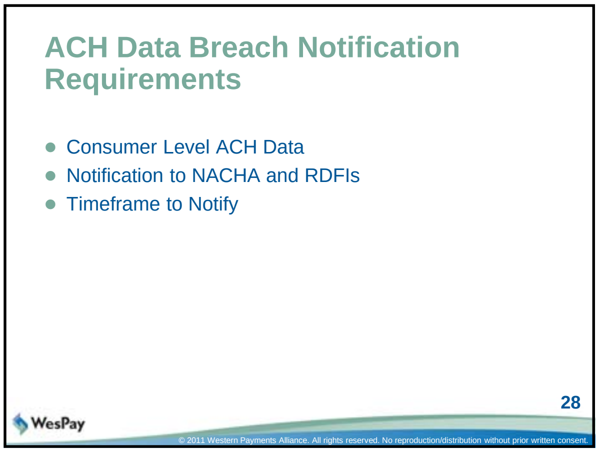


Incident Reporting

- File a police report
- FS-ISAC (Financial Services – Information Sharing & Analysis Center) recommends:
  - FS-ISAC Suspicious Incident Report
- FBI recommends
  - Call FBI
  - www.fbi.gov
  - Report to Internet Crime Complaint Center
  - www.ic3.gov
- File a SAR when required

27

WesPay



ACH Data Breach Notification Requirements

- Consumer Level ACH Data
- Notification to NACHA and RDFIs
- Timeframe to Notify

28

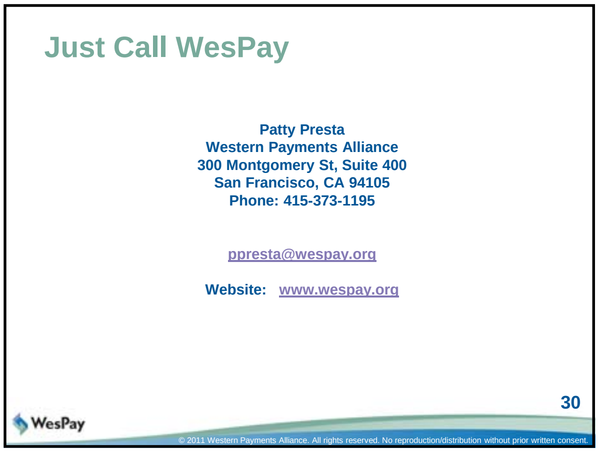
WesPay

Case Law Examples

- Patco Construction v. Ocean Bank
  - (“Commercial Reasonableness” of Security Procedures”)
- Experi-Metal v. Comerica
  - (Duty to Prove “Good Faith”)

29

WesPay



Just Call WesPay

Patty Presta
Western Payments Alliance
300 Montgomery St, Suite 400
San Francisco, CA 94105
Phone: 415-373-1195

ppresta@wespay.org

Website: www.wespay.org

30

WesPay