

EXAMPLES OF POTENTIAL THREATS

Consider threats/vulnerabilities to assets that could create risk to NPI (non-public information) or customer financial transaction information.

General Threats: Unauthorized Access that could affect data integrity, data confidentiality, system/data availability; Data destruction/loss; loss of productivity, inaccessibility to non-public information (NPI) assets, financial transaction loss.

Includes references to the threats in the *FFIEC Authentication in an Internet Banking Environment (2005) and Guidance Supplement (2011)*. *See Technology Based Threats section below

Non- Technology Based Threats:

Unauthorized disclosure due to files/customer information left on desk
Computer monitors viewable by outsiders
E-mails containing customer information or references sent to the wrong recipients
Disgruntled employee
Items left on the fax machine
Natural disasters
Failure to secure vault
Information given to unauthorized persons by phone
Records misfiled
Account hijack of customer's info through Internet Banking
Unauthorized access physical access –threat to electronic
Lost reports containing sensitive data
NPI found in regular trash
Unlocked file cabinets
Unauthorized access of facility after hours may access sensitive confidential information;
Access
to unauthorized areas of bank – customer information threat (visitors in bank)
Phishing incident
Lap top/PDA stolen
Janitor stealing
Courier bag destroyed/lost
Loose lips (employee unintentional)

Technology Based Threats: *Includes system misuse and/or access to NPI and financial transaction data resulting in account takeover for malicious intent (facilitating unauthorized movement of funds).*

Keylogging malware

MIM or MIB malware attacks

Money Mule Schemes

Unauthorized access to the bank's core systems via the Internet

Unauthorized access to information or systems (vendors, employees, intruders)

Unauthorized access to electronic records/reports which may be obtained by vendors, current or previous employees or intruders.

"Unknown" items installed; untested or unstable programs

Hacker access through firewall

Former users not removed from system

Data attacks (viruses, worms, spam, hoaxes, Trojan horses, phishing, smishing, vishing, war driving, etc)

Data compromise, theft and/or disclosure

Data loss

Interception of data through wireless network, Internet

Security patches inadequate (can create vulnerabilities)

System/data inaccessibility, unavailability, disruption, loss or damage due to hardware failure, natural disaster, pandemic flu, data corruption, invalid backups, infrastructure disruptions (electrical power or telecommunications failure)

Data storage devices utilized for fraudulent purposes (copied NPI to take out of the bank)

Back up media lost or stolen

ATM Skimming