CAMPUS FEDERAL®

Baton Rouge • New Orleans • Shreveport

campusfederal.org

HANDLING ACH PROTECTED INFORMATION

	Paper Documents	Electronic Formats – Password protected, Encrypted or Masked
How is Protected Information collected?	• Authorization forms • Corporate Trade agreements • Applications • Origination Agreements • Set-Up/On-Boarding documents	• Internet Initiated authorizations • Telephone/ORV/VRU authorizations • Mobile authorizations
Where is Protected Information stored?	• Locked cabinets or drawers	• Secure servers, desktops and laptops • USB drives, CDs • Secure online websites or cloud-computing

MOVING ACH PROTECTED INFORMATION

How is Protected Information moved, or transmitted, for initiation into the ACH network?	To ODFI: • Via Online Banking • Via Secure File Transmissions – FTPS • Hand-delivery of CD or USB drive To Third-Parties for processing • Via secure online website • Via secure email Does the Corporate customer adhere to the Security Procedures for Transmissions as established by the ODFI?
What devices are used to access Protected Information?	• Desktops • Laptops • Remote Access • Mobile Devices • CD or USB drives
Are devices secured?	• Up-to-date anti-virus • Anti-malware/spyware • Encryption software
Who has approved access to Protected Information?	• Employees • ODFI • Third-Parties

DESTROYING ACH PROTECTED INFORMATION

	PAPER DOUMENTS	ELECTRONIC FORMATS – PASSWORD PROTECTED, ENCRYPTED OR MASKED
Is Protected Information destroyed in a secure manner?	• Shredded	• Data erased • Wiped

OTHER CONSIDERATIONS

Minimize or destroy information that is not needed.	
Use effective passwords	• Never use default passwords • Use strong passwords or password phrases that is unique to each user - Specific length and character type - Specify how password should be kept secure • Do not share password with co-workers • Change password frequently • Use password-activated screensavers • Safeguard passwords
Block Potential Intruders	• Restrict use of computer for business purposes only • Protect your IT system – anti-virus/spyware software, firewalls • Limit or disable unnecessary workstation ports/services/devices • Automatic log-outs after a certain amount of inactivity • Change all vendor supplied passwords (administrator account in particular) • Encrypt all data when moved and when stored • Install updates as soon as it published • Log off computer or device when not in use
Restrict Access	• Limit the number of locations where Protected Information is stored • Keep paper records in locked cabinet • Limit employee access to Protected Information, including server rooms • Take precaution when mailing Protected Information • Encrypt or mask electronic Protected Information • Do not store Protected Information on portable devices • Transmit Protected Information over the Internet in a secure session • Establish an Internet Acceptable Usage Policy
Educate Staff	• Keep Protected Information safe and secure at all times • Mask Protected Information in communications, such as phone calls, emails and postal mail • Make staff aware of security policy • Make staff aware of phishing scams, via emails or phone calls • Notify staff immediately of potential security breach • Establish a Clean Desk Policy

ACH STANDARD ENTRY CLASS CODES / TYPES OF PROCESSING

CODE	NAME	DESCRIPTION	ACCT/MARKET TYPE	TRANSACTION TYPE	CREDIT/DEBIT
CCD	Corporate Credit/Debit Entry	Funds are transferred between unrelated corporate entities or transferred as intra-company cash concentration and disbursement transactions. Proof of Authorization for transactions ran on the web using CCF will adhere to the same requirements as a web transaction.	• Non-Consumer • Retail, Phone, Order, Ecommerce and Mail Order	Single or Recurring Entry	Credit / Debit
PPD	Prearranged Payment and Deposit Entry	Credit – A single or recurring credit transaction for payment of payroll, expense reimbursement, dividends, retirement, interest, etc. Debit – A single or recurring debit transaction for collection of fixed or variable amounts for loan and mortgage payments, utilities, insurance, tuition, contributions, etc.	• Consumer • Mail Order and Retail	Single or Recurring Entry	Credit / Debit
WEB	Internet-Initiated Entry	Credit – A single or recurring credit transaction from the account of a natural person to the account of a natural personal. Cannot be used for business – to – consumer transactions. Debit – A single or recurring debit transaction initial during a secure (minimum 128 -bit encryption) internet or mobile session.	• Consumer • Ecommerce	Single or Recurring Entry	Credit / Debit