craft bank

2nd QUARTER 2025

PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

Why Business Owners Must Take User Access Seriously

Assigning the ability to transmit funds is not a decision that should be taken lightly. Business owners must recognize that granting this level of access effectively gives the user control over the company's financial resources. Without proper oversight and safeguards in place, this access can be exploited — either intentionally or unintentionally — to the detriment of the business.

Knowing the Difference between a Signer on an Account and an Authorized User - The key difference between a signer and an authorized user in cash management lies in the level of authority and responsibility:

Role	Authority
Signer on Account	A signer has legal authority over the account. They can make critical decisions such as adding or removing users, changing account details, or closing the account. Signers are legally responsible for the account's activities and bear ultimate responsibility for its management.
Authorized User	An authorized user is granted access to perform specific tasks within the cash management system, such as initiating transactions (e.g., ACH, wire transfer and Bill payments) or viewing account information.

Business owners often confuse these two roles and may not fully understand the authority and risks involved in granting user access, including the extent of actions a user is authorized to perform.

Key risk considerations for business owners include:

- **The Potential for Withdrawing Unauthorized Funds:** If an authorized user can send funds without oversight, they could empty the account in a matter of minutes. This could be due to fraud, mismanagement, or even errors like sending funds to the wrong recipient.

- **Accountability and Oversight:** Owners should be actively involved in approving user access and establishing internal controls. This includes setting clear limitations on what an authorized user can do and regularly monitoring their activity.

- **The Cost of Negligence:** Beyond financial losses, mismanagement of user access can lead to reputational damage, loss of trust with vendors or clients, and potential legal consequences if funds are misappropriated.

Protecting Your Account

There are controls you can implement to help in the protection of unauthorized access to your account. These include but are not limited to the following:

- **Define Roles and Permissions** - Before granting access, clearly define each user's tasks and assign only the necessary permissions. Limit access to sensitive functions, like fund transfers, unless absolutely required.

- **Implement Dual Control and Approval Workflows** - For high-risk transactions, such as wire transfers or ACH payments, require dual control, where one user initiates the transaction, and another approves it. This ensures no single user has unchecked authority over company funds. Ensure users are prohibited from sharing dual control access (e.g., one employee provides their account login to another employee).

- **Regularly Review User Access** - Periodically review all authorized users and their permissions. Remove

access for users who no longer require it or whose roles have changed.

- **Provide Training -** Ensure that authorized users understand their roles, the extent of their permissions, and the importance of maintaining security and compliance.

- **Perform Daily Reconcilement** – Access your online banking system and review account activity, flag suspicious behavior, and report to us immediately.

- **Establish Strong Internal Controls** - Develop policies and procedures for granting, monitoring, and revoking user access. Ensure these controls are consistently followed and updated as needed.

Granting authorized user access to cash management systems is essential but risky. Without proper controls, it can lead to financial losses, data breaches, or compliance issues. Clear controls, limited permissions, and regular reviews are key to safeguarding resources and ensuring security.

Upcoming Changes to Regulation CC

Exciting updates are coming to Regulation CC that will impact the way banks handle funds availability for their customers. As required by the Expedited Funds Availability Act (EFAA), the Consumer Financial Protection Bureau (CFPB) and the Federal Reserve Board (FRB) — jointly referred to as "the Agencies" — have announced final cost-of-living adjustments (COLAs) to the dollar amounts outlined in the regulation's funds availability rules.

Here's what's changing: We are increasing the amount we make available for withdrawal by checks not subject to next-day availability to $275. In addition, the amount available for withdrawal on exception holds for large deposits, new accounts, and the amount for determining a repeat overdraft is increasing to $6,725.

If you have any questions regarding these changes, please contact us for assistance.

The Importance of Fraud Procedures:

Get prepared for upcoming Nacha Rules Changes and Business Email Compromise - Fraud prevention has never been more critical, and Nacha's upcoming amendments to its Risk Management Rules highlight the importance of proactive measures.

Business email compromise (BEC) is one of the fastest-growing cyber threats, targeting organizations of all sizes. This sophisticated type of fraud involves cybercriminals gaining access to or impersonating legitimate business email accounts to manipulate employees, customers, or vendors into transferring funds or sensitive information.

BEC attacks typically rely on social engineering methods. Scammers study an organization's communication patterns and impersonate trusted individuals, such as executives, vendors, or partners, to send fraudulent requests.

Common Fraud Tactics

Invoice Fraud	Impersonating a vendor to request payment to a fraudulent account.
CEO Fraud	Pretending to be a company executive and requesting urgent wire transfers.
Payroll Diversion	Tricking HR or payroll staff into redirecting direct deposit payments to a scammer's account.

These attacks are often carefully crafted to appear legitimate, making them difficult to detect without proper safeguards in place.

Steps to Protect Your Business

Preventing BEC begins with awareness and proactive measures. Here are key steps to safeguard your organization:

- **Train staff** to recognize phishing emails, suspicious requests, and urgent demands for financial transactions.

- **Implement strict protocols** for verifying payment requests, especially those involving changes to account details or large sums of money.

- **Use email filtering and monitoring** tools to identify unusual activity or messages.

- **Encourage employees to report suspicious emails or transactions immediately** and have a clear plan for incident response.

Take Action Today!

By prioritizing fraud prevention, ACH Network participants can protect their customers, reduce unauthorized transactions, and contribute to a more secure payments ecosystem.

If you have questions about the newsletter or would like more information on fraud mitigation tools and treasury service offerings, please contact:

CRAFT BANK
SUPPPORT@CRAFT.BANK
678-736-5060