Online security for better business banking

Protect your business from potential fraud

October 2020

U.S. Bank Global Treasury Management

Today's presenters

Nina Hanselmann

Working Capital
Consultant,
U.S. Bank

Nidhi Gupta

Digital Channels
Product Manager,
U.S. Bank

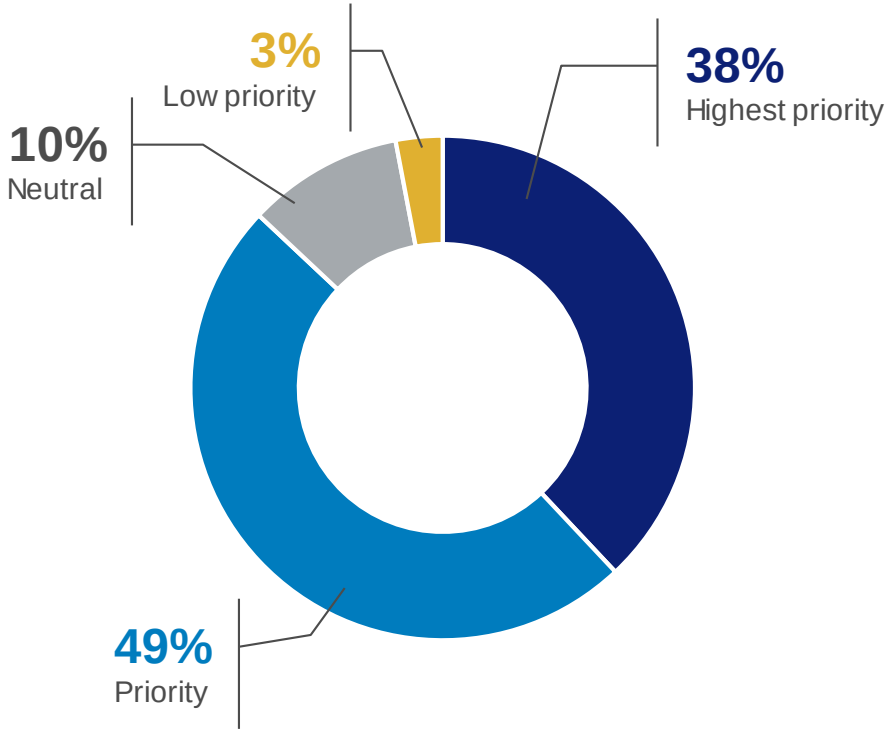
Chris Halloran

SinglePoint Training
Content Developer,
U.S. Bank

What practitioners are saying

Top of Mind

Level of priority treasury and finance functions place on cybersecurity, relative to the other challenges.[1]



88% were victims to actual or attempted cyberattacks in the prior 18 months.[1]

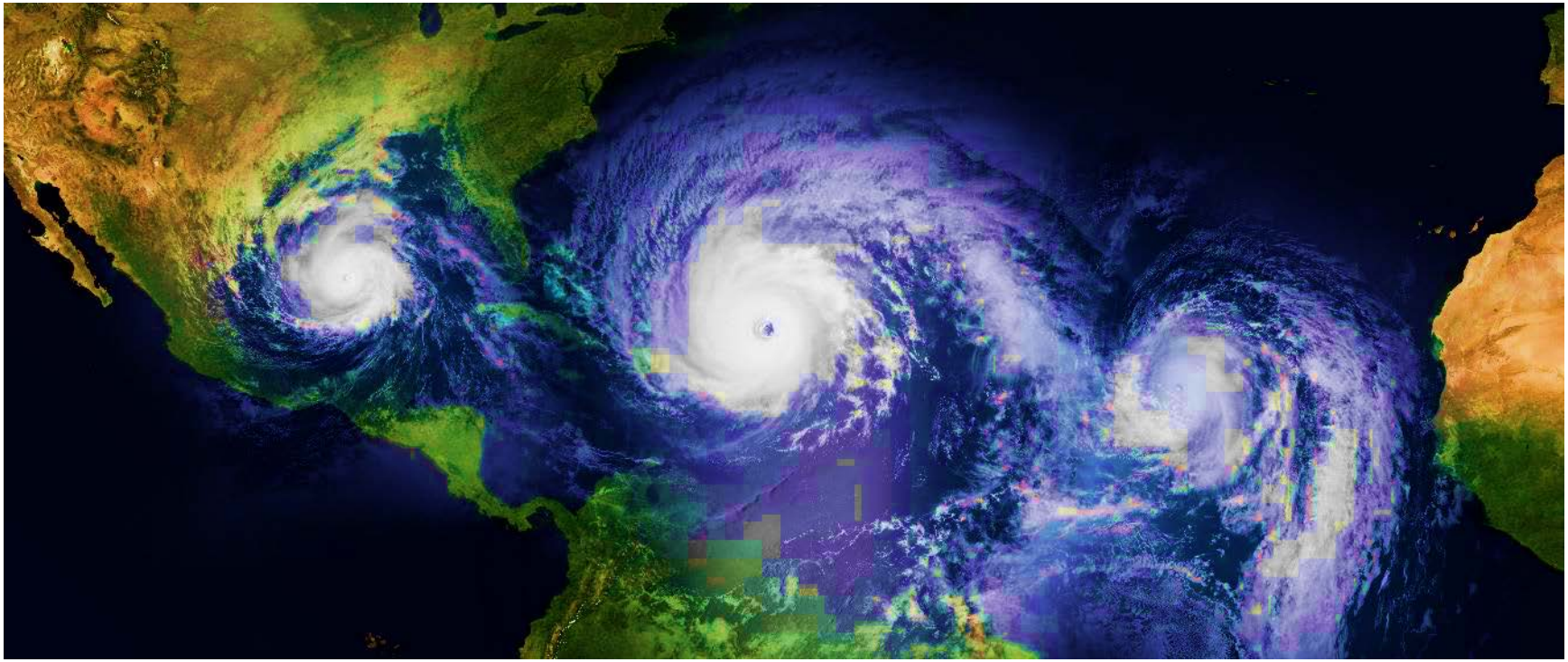
82% expect cyberattacks involving financial and data theft to increase.[1]

80% predict disruption to their business operations.[1]

1. 2019 annual conference for the Association for Financial Professionals (AFP).

The perfect storm for fraud

- Employee turnover
- Disrupted communication patterns
- Transition to remote workforce
- Competing priorities

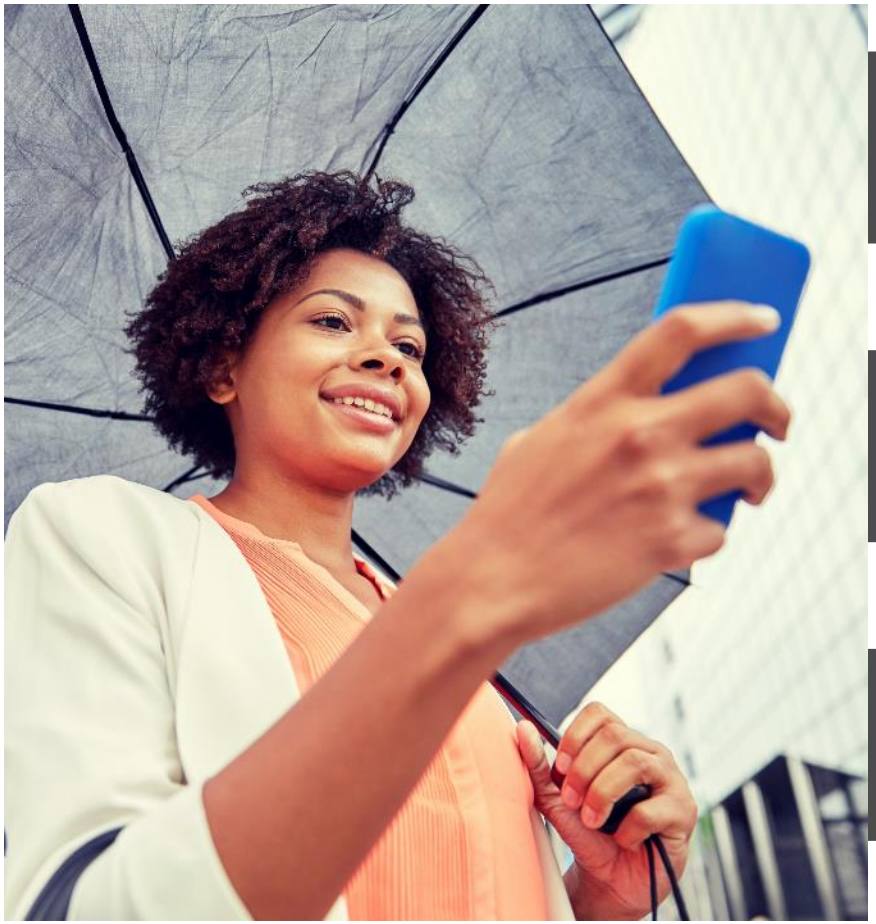


Managing your security is challenging

What you told us…

- Cumbersome
- Hard to get a full overview
- What are the right settings?

Designing a new tool for you



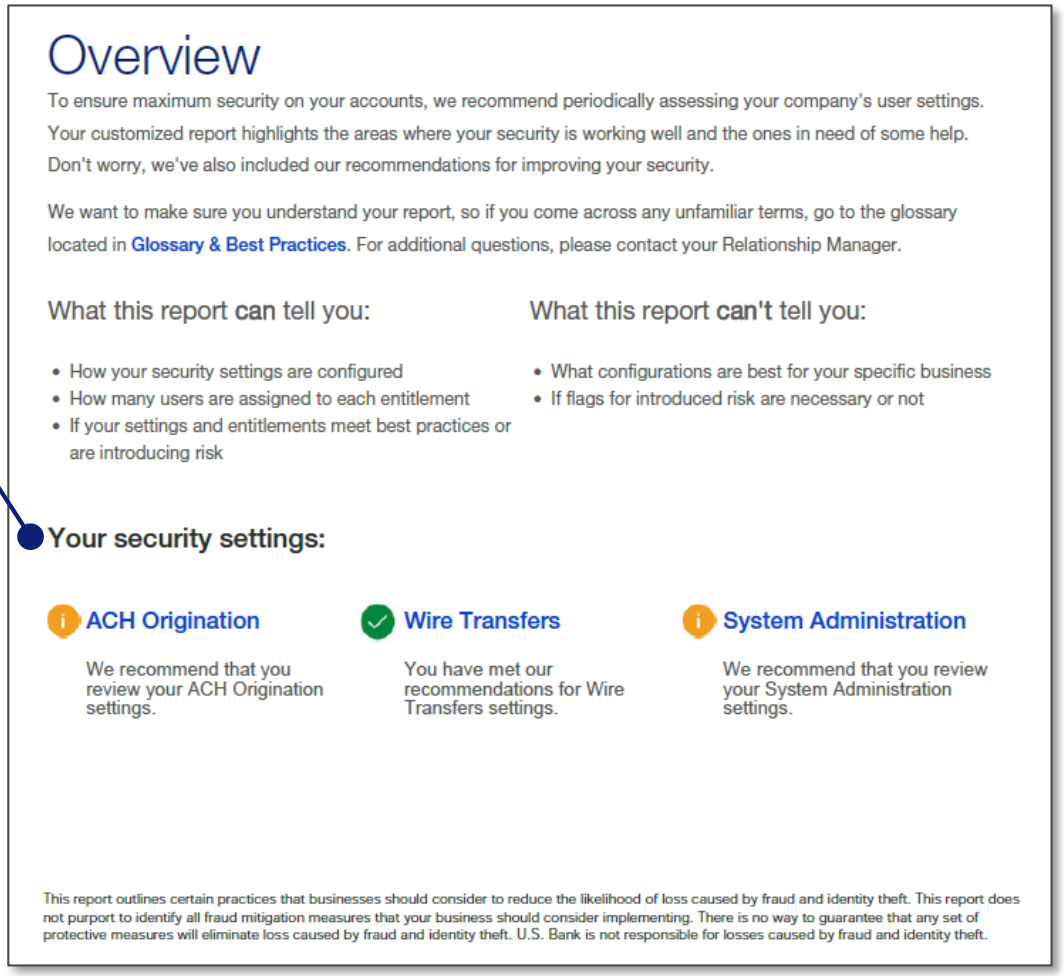
Pull all information into one space to evaluate

intuitive and simplified

Framework to provide insight and recommendations

SinglePoint Security Settings Report

Visibility on your main payment and System Administration related settings to mitigate risk.



Overview

To ensure maximum security on your accounts, we recommend periodically assessing your company's user settings. Your customized report highlights the areas where your security is working well and the ones in need of some help. Don't worry, we've also included our recommendations for improving your security.

We want to make sure you understand your report, so if you come across any unfamiliar terms, go to the glossary located in **Glossary & Best Practices**. For additional questions, please contact your Relationship Manager.

What this report **can** tell you:

- How your security settings are configured
- How many users are assigned to each entitlement
- If your settings and entitlements meet best practices or are introducing risk

What this report **can't** tell you:

- What configurations are best for your specific business
- If flags for introduced risk are necessary or not

Your security settings:

ACH Origination

We recommend that you review your ACH Origination settings.

Wire Transfers

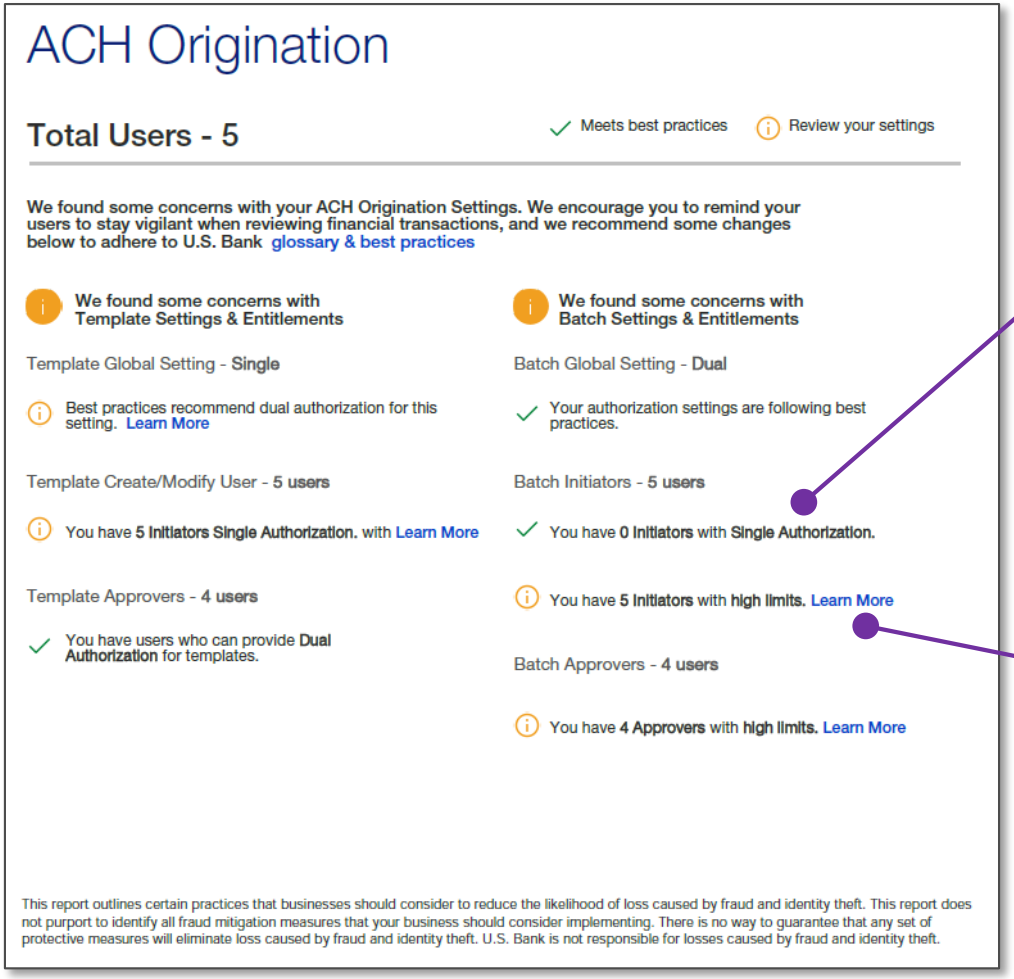
You have met our recommendations for Wire Transfers settings.

System Administration

We recommend that you review your System Administration settings.

This report outlines certain practices that businesses should consider to reduce the likelihood of loss caused by fraud and identity theft. This report does not purport to identify all fraud mitigation measures that your business should consider implementing. There is no way to guarantee that any set of protective measures will eliminate loss caused by fraud and identity theft. U.S. Bank is not responsible for losses caused by fraud and identity theft.

Payment Origination Pages



ACH Origination

Total Users - 5

Meets best practices | Review your settings

We found some concerns with your ACH Origination Settings. We encourage you to remind your users to stay vigilant when reviewing financial transactions, and we recommend some changes below to adhere to U.S. Bank glossary & best practices

We found some concerns with Template Settings & Entitlements

Template Global Setting - **Single**

Best practices recommend dual authorization for this setting. Learn More

Template Create/Modify User - **5 users**

You have **5 Initiators Single Authorization.** with Learn More

Template Approvers - **4 users**

You have users who can provide **Dual Authorization** for templates.

We found some concerns with Batch Settings & Entitlements

Batch Global Setting - **Dual**

Your authorization settings are following best practices.

Batch Initiators - **5 users**

You have **0 Initiators** with **Single Authorization.**

You have **5 Initiators** with **high limits.** Learn More

Batch Approvers - **4 users**

You have **4 Approvers** with **high limits.** Learn More

This report outlines certain practices that businesses should consider to reduce the likelihood of loss caused by fraud and identity theft. This report does not purport to identify all fraud mitigation measures that your business should consider implementing. There is no way to guarantee that any set of protective measures will eliminate loss caused by fraud and identity theft. U.S. Bank is not responsible for losses caused by fraud and identity theft.

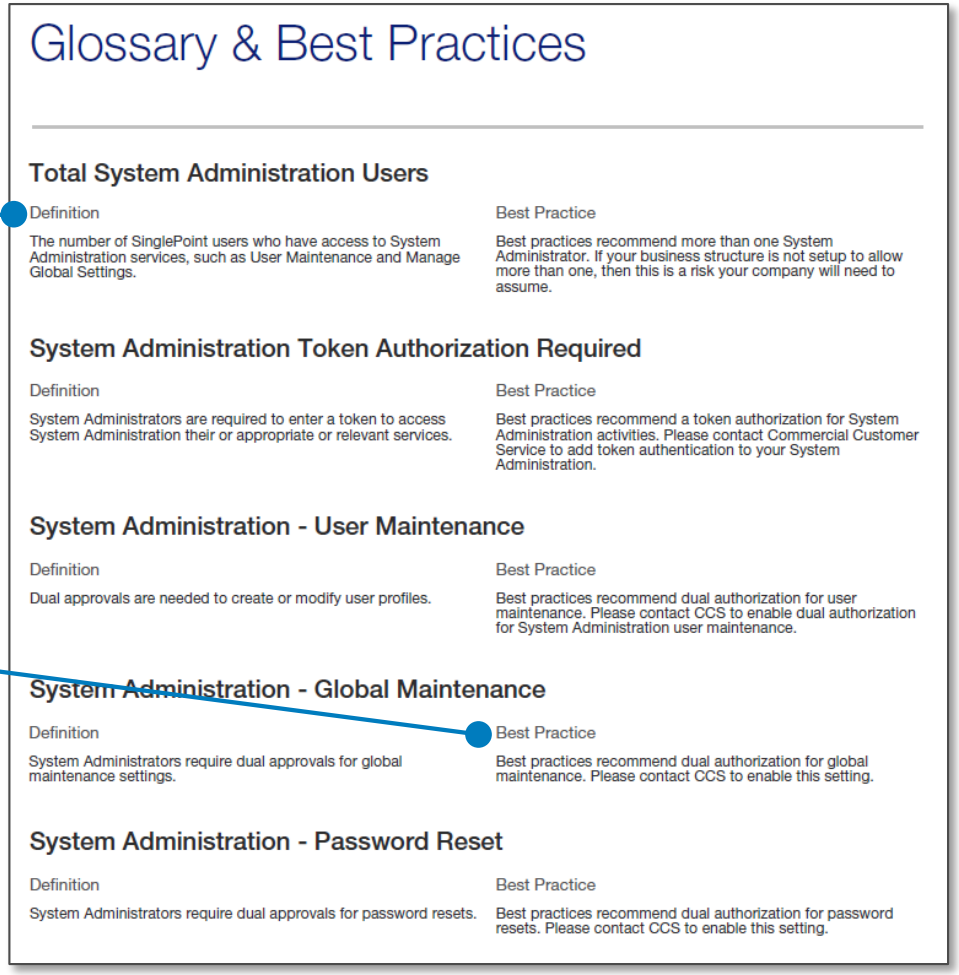
Identify areas where you are meeting best practices.

Outlines opportunities for improvements.

Best Practices

Glossary defines SinglePoint security terminology.

Recommendations to improve your security.



Glossary & Best Practices

Total System Administration Users

Definition	Best Practice
The number of SinglePoint users who have access to System Administration services, such as User Maintenance and Manage Global Settings.	Best practices recommend more than one System Administrator. If your business structure is not setup to allow more than one, then this is a risk your company will need to assume.

System Administration Token Authorization Required

Definition	Best Practice
System Administrators are required to enter a token to access System Administration their or appropriate or relevant services.	Best practices recommend a token authorization for System Administration activities. Please contact Commercial Customer Service to add token authentication to your System Administration.

System Administration - User Maintenance

Definition	Best Practice
Dual approvals are needed to create or modify user profiles.	Best practices recommend dual authorization for user maintenance. Please contact CCS to enable dual authorization for System Administration user maintenance.

System Administration - Global Maintenance

Definition	Best Practice
System Administrators require dual approvals for global maintenance settings.	Best practices recommend dual authorization for global maintenance. Please contact CCS to enable this setting.

System Administration - Password Reset

Definition	Best Practice
System Administrators require dual approvals for password resets.	Best practices recommend dual authorization for password resets. Please contact CCS to enable this setting.

On the horizon

Evaluate & buy	Connect	Implement	Transact	Optimize
solutions tailored to your needs	easily and seamlessly	quicker and track digitally	faster and in more ways	using data and industry trends

See end disclosures.

More information on fraud?

Checklist

Fraud prevention checklist

Article

4 tips for protecting your business against Coronavirus-related scams

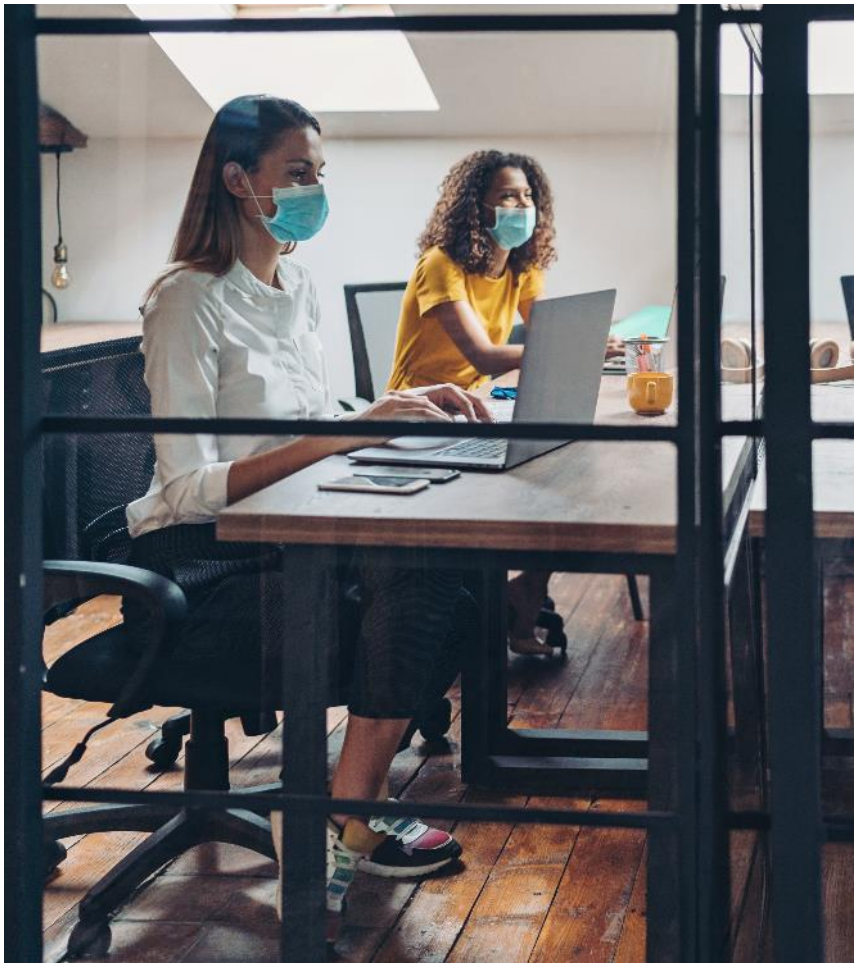
Article

Stop payments fraud in its tracks

Check out our Minimize Risk page on Financial IQ:

https://www.usbank.com/financialiq/improve-your-operations/minimize-risk.html

Join us for December's webinar



Driving innovation for impact

Thursday, December 10

11 a.m. PT, noon MT

1 p.m. CT, 2 p.m. ET

Learn more at Financial IQ:
https://financialiq.usbank.com/index.html

Follow us on LinkedIn:
https://www.linkedin.com/showcase/corporate-and-commercial-banking/about/

See end disclosures.

Disclosures