People's United Bank® What know-how can do®

Emerging Payment Fraud Threats

FAST FACTS AND TIPS

Fraudsters are constantly finding new, creative ways to attack businesses. Learn how to stay one step ahead.

What's Driving Change?

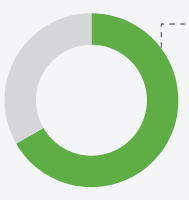
THE COVID-19 PANDEMIC

79% of anti-fraud experts have **seen fraud increase across all categories** since the pandemic began.

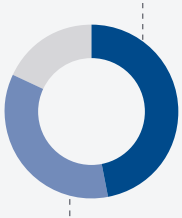
72% are seeing an **increase in payment fraud.**

82% anticipate payment fraud **will continue to increase over the next 12 months.**[1]

WORK-FROM-HOME CULTURE



Nearly two-thirds of U.S. workers who have been working remotely during the pandemic would like to continue to do so.[2]



82% of business leaders say their companies **will continue to permit part-time remote work for employees.**

Nearly half **(47%)** will permit full-time remote work.[3]

[1] ACFE *Fraud in the Wake of COVID-19: Benchmarking Report*, December 2020

[2] Gallup: *COVID-19 and Remote Work: An Update*, October 13, 2020

[3] Gartner, *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time*, July 14, 2020

How Can You Reduce Risk?

1. REVIEW YOUR EMPLOYEE TRAINING

38% of small companies + **28%** of large companies **have not implemented training with a testing component for employees involved in payments.**[4]

Social engineering is also on the rise and targeting employees.

98% of cyberattacks rely on social engineering.[5]

And, **60% of IT professionals cite recent hires as being at high risk for social engineering.**[6]

Employees can be a strong line of defense against fraud. It's critical to keep them informed and involved in fraud prevention.

- Require fraud prevention and detection training for all employees. Include a testing component to ensure comprehension.
- Regularly send employees fraud and risk communications so they are aware of emerging threats.
- Review your fraud reporting processes. Identify areas to improve or streamline so it's easy for employees to report.

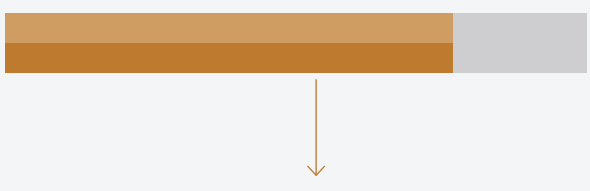
[4] TD Bank and Strategic Treasurer, *2020 Treasury Perspectives: Survey Report*, 2020.

[5] Guardian Digital, *Think Like a Criminal: What You Need to Know About Social Engineering Attacks in 2020*, September 25, 2020

[6] Data Insider, *Social Engineering Attacks: Common Techniques and How to Prevent an Attack*, December 1, 2020

2. ASSESS YOUR FRAUD PREVENTION TECHNOLOGY

Fraud is growing. **73% of organizations think the threat level of fraud has increased in the past year.**[7]



But the pandemic has created new fraud opportunities as financial and health threats emerge.

Companies must now be prepared for threats resulting from changed business processes, such as fast-tracking new business partners and suppliers.[8]

- Review the vetting and screening process for onboarding third parties, suppliers, etc. Identify potential gaps during the process and address them.
- Leverage online entitlement controls for proper separation of duties and "need only" access for employees.
- Verify all requests for bank account changes with known contacts before sending any payments.

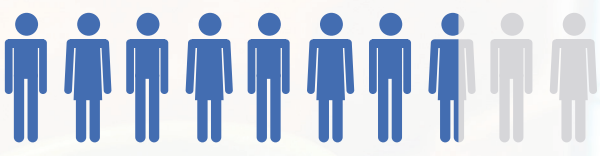
[7] AFP, *2020 AFP Payments Fraud and Control Survey*, 2020

[8] Deloitte, *COVID-19 Operating in the 'New Normal'—A Backdoor to Increased Fraud Risk?*

3. STRENGTHEN YOUR ONLINE TOOLS

Many businesses will have employees working remotely out of public health concerns for the foreseeable future.

But **77% of anti-fraud experts** say that **fraud prevention and fraud investigations are more challenging** as remote work continues.[9]



Confirm that your online tools are doing what they're supposed to do in identifying and investigating potential fraud threats—and that your remote employees can leverage those tools to protect themselves against fraud and bad actors.

- Identify processes that require in-person approvals and create alternative workflows within your online tools. This may include converting fraud-prone paper check payments to electronic methods.
- Confirm that your tools and processes support any paper trails you've digitized. These digitized paper trails should help you during audits.
- Ensure your systems and data from your tools are regularly backed up, and that the backups can be accessed in the event of security threats or incidents.

[9] ACFE *Fraud in the Wake of COVID-19: Benchmarking Report*, December 2020

Fraud threats are constantly growing and changing. A defined, thoughtful, and proactive approach to payment security is a critical component in any business strategy.

Check out our treasury management resource center to gain more actionable insights.

www.peoples.com/getstreamlined