

7 BANKING FRAUD MYTHS ***BUSTED***

JUNE 17, 2021

Meet the Presenters



Andy Shank

VP, Fraud and Risk Product Management
Harland Clarke, a Vericast Business

andy.shank@harlandclarke.com

- 18+ years experience assessing risk and investigating fraud, at the local, state and federal level, across multiple sectors
- Former Indiana State Police detective assigned to the FBI to investigate white-collar crime and public corruption
- Featured on CNBC's *American Greed* for his investigation of a high-profile federal criminal fraud case



Kellyn Burns

VP, Financial Institutions &
Strategic Partnerships,
Sontiq

kburns@sontiq.com

- 10+ years of experience helping financial institutions tackle security challenges
- Expertise includes cybersecurity and fraud solutions, data breach management, digital transformation, and business security solutions
- Partners with financial institutions to combat fraud and protect account holders from the effects of data breaches, cybercriminals, and identity theft

A person wearing a dark hoodie is shown from the chest up, with their hands raised in front of them. The image is overlaid with a complex, glowing blue digital circuitry pattern, suggesting a theme of technology, hacking, or digital security.

81%

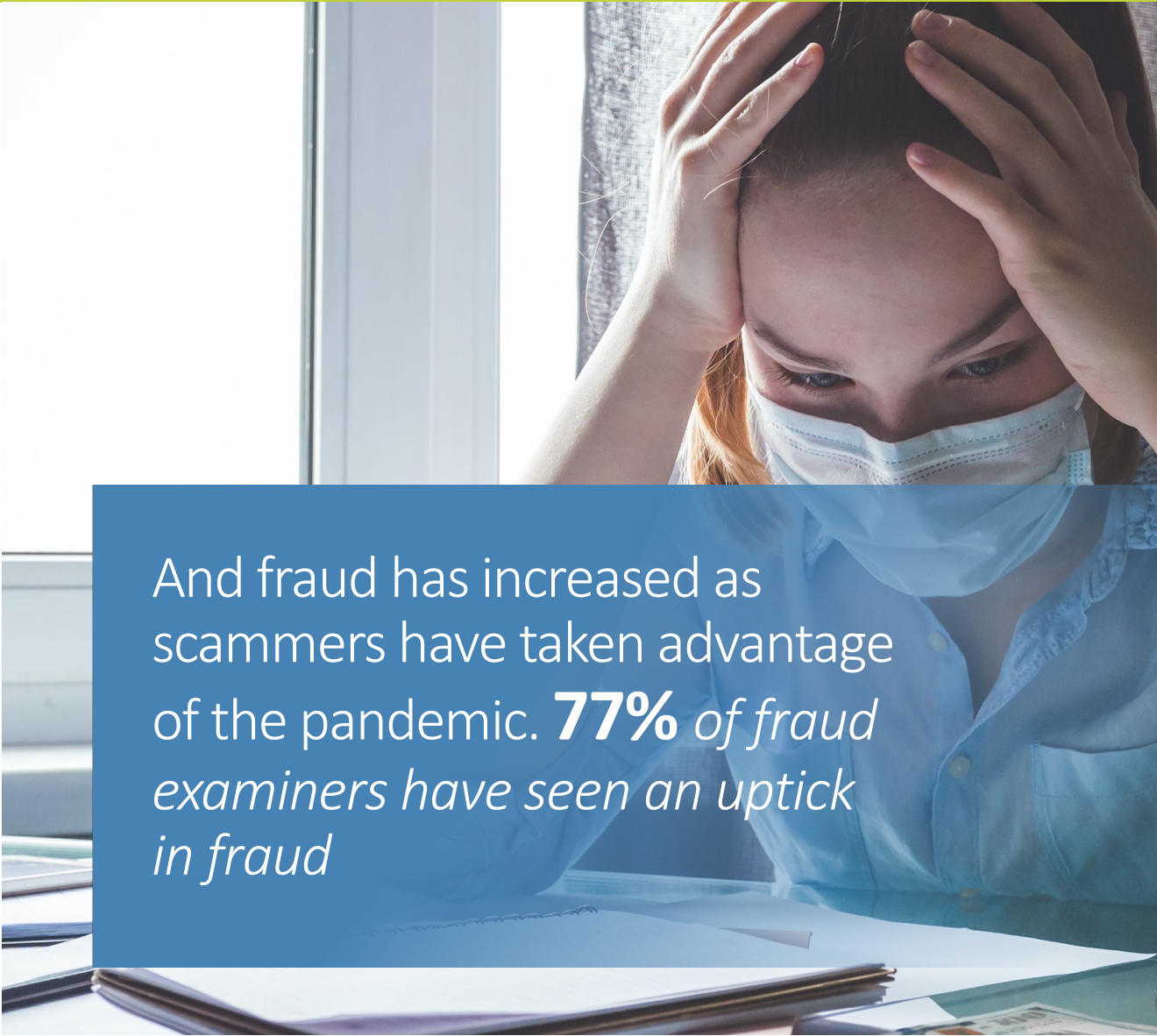
OF FINANCIAL PROFESSIONALS
REPORT THEIR ORGANIZATIONS
HAVE BEEN VICTIMS OF ATTEMPTED
OR ACTUAL FRAUD¹

WHAT WE'LL DO TODAY:

- Gain a clear understanding of fraud today
- Learn best practices on how to defend against fraud
- Know what's available in fraud protection technology

As banking technology becomes more sophisticated, so do fraudsters.

- Highly synchronized
- Creative and sophisticated
- Bold



And fraud has increased as scammers have taken advantage of the pandemic. **77%** of fraud examiners have seen an uptick in fraud

Let's Bust Some *Common Fraud Myths!*

myth #1:

All credit unions really need to
worry about is **check
fraud.**

fact #1:

PHISHING AND ONLINE BANKING
VULNERABILITIES ARE GROWING
OPPORTUNITIES FOR
FRAUDSTERS.

Banking has overtaken retail as
the 3rd most likely industry targeted
by hackers seeking to acquire and
misuse personal information.

myth #2:

Once your online / mobile banking platform is up and running, you can
“set it and forget it.”

fact #2:

ONLINE BANKING AND MOBILE
APP PLATFORMS REQUIRE
FREQUENT MAINTENANCE AND
SECURITY REVIEW.

22% of consumers would use mobile deposit capture more frequently if they had better assurance that their checks had been deposited securely.

myth #3:

Fraud prevention strategies
are too costly; **it's overkill.**

fact #3:

INVESTING IN FRAUD PREVENTION PAYS FOR ITSELF.

Community banks spend between \$10,000 and \$50,000 on anti-fraud investments. In the financial industry, the average data breach costs \$5.9M.

myth #4:

Once you've resolved an account takeover incident **you're less vulnerable** to future attacks.

fact #4:

IF YOU ARE TARGETED IN AN
ACCOUNT TAKEOVER, YOU ARE
MORE LIKELY TO BE TARGETED A
SECOND OR THIRD TIME.

89% of financial institution
executives believe ATOs are the most
common fraud in the digital channel.

myth #5:

Addressing fraud at the account level
is sufficient.

fact #5:

ACCOUNT EXPOSURE IS ONLY ONE
PART OF THE EQUATION — THE
PERSON RECEIVING THE ORDER IS
OFTEN THE PAWN, NOT THE
MASTERMIND OF THE CRIME.

A large group working toward
organized fraud can do more
financial damage than any
individual fraudster ever will.

myth #6:

There is not much you can do to minimize
the effect of identity fraud; it's mostly about
**“cleaning up”
the aftermath.**

fact #6:

FRAUD PREVENTION SOLUTIONS
CAN DELIVER NOTIFICATIONS
WHEN ACCOUNTS HAVE BEEN
COMPROMISED, PROVIDING AN
OPPORTUNITY TO LIMIT THE EFFECTS.

Companies that invested in fraud prevention incurred lower costs when a fraud was experienced.

myth #7:

Periodic fraud training for staff
isn't worth **the investment.**

fact #7:

**YOUR STAFF IS YOUR FIRST LINE
OF DEFENSE AGAINST FRAUD.**

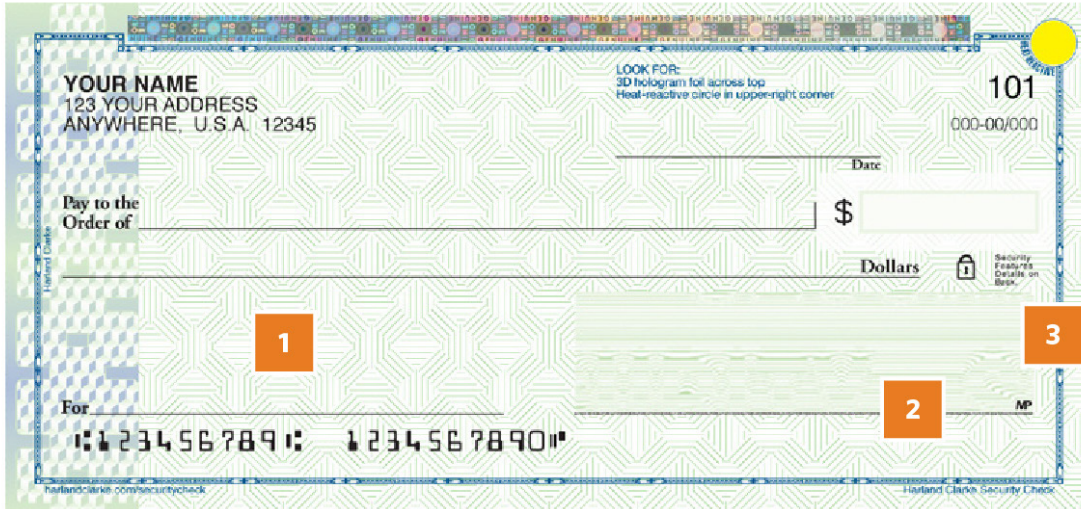
**There is more than a 25% chance
that a user will mistakenly click on
a phishing email and infect
corporate network.**

POLL QUESTION

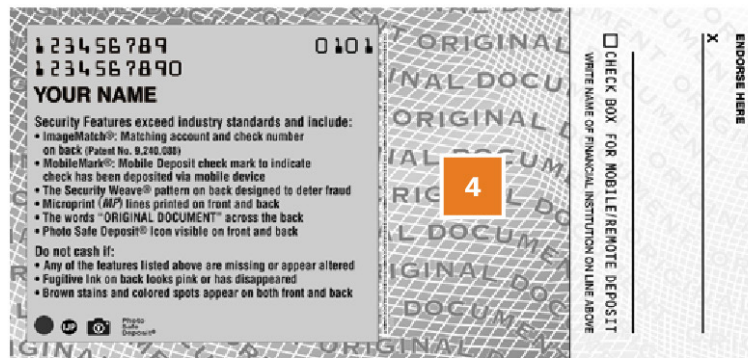
How would you describe your current fraud prevention strategy?

- A. We don't have one.
- B. We leave fraud prevention responsibilities to our members.
- C. We have one, but it needs improvement.
- D. We have an effective fraud prevention strategy.

Check Security



High Security Personal Check - front



Standard Personal Check - back

1 Check background pattern and security safety paper make stains appear if common chemicals are used to change the original information on the check.

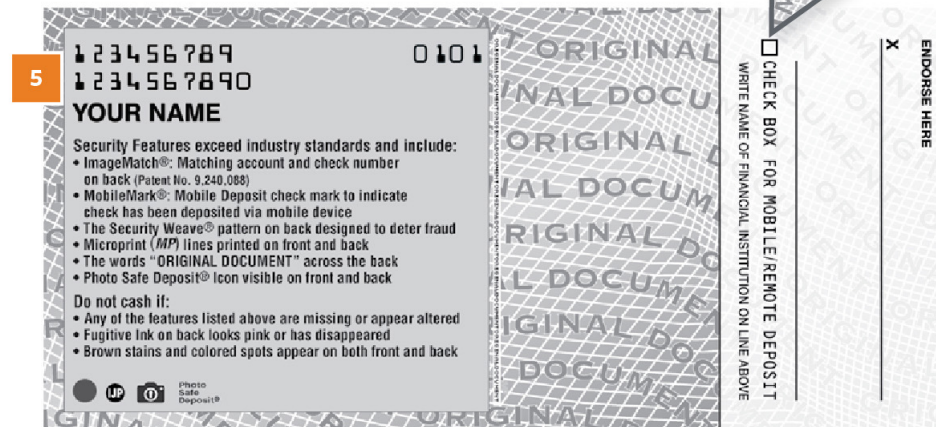
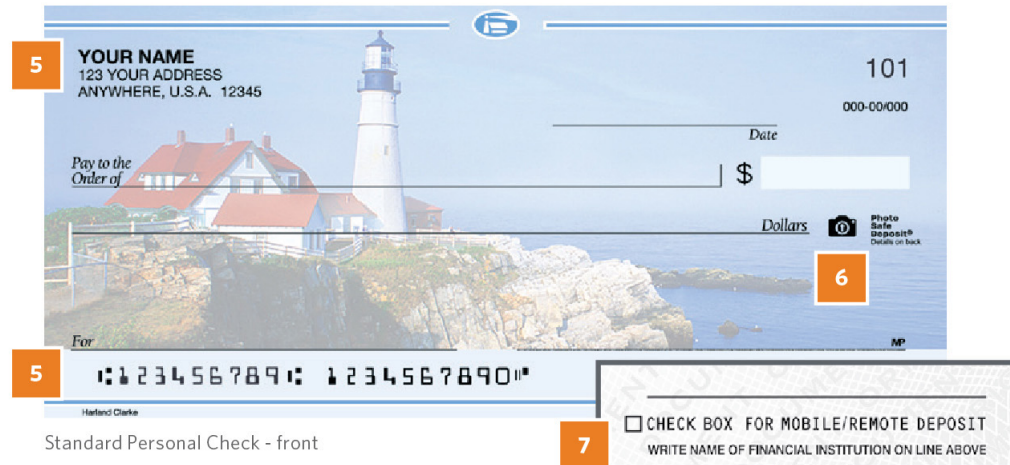
2 Microprint is a fine line of type on the check that can be read when magnified, and it is very difficult to photocopy.

3 This high-resolution border is so uniquely designed it is difficult to replicate and often distorts when copied.

4 The security screen ensures the words “Original Document” will fade, distort or disappear if a check is copied or scanned by traditional means.

Mobile Deposit Security

Security technology is about more than what's on our phones and screens.



5 **ImageMatch®** helps prevent fraud by confirming unique check information such as account number and routing number match the front and back of the check.

6 The **Photo Safe Deposit®** icon indicates that check includes mobile deposit fraud prevention features.

7 The **MobileMark®** box printed on the back of the check helps customer keep track of checks deposited remotely.

Fraud prevention best practices

- Train branch staff on how to identify and prevent fraud, and how to speak to members about fraud
- Arm members with the education, tools and information they need to prevent fraud and encourage them to protect themselves
- Ensure your checks and other payment tools offer industry-leading security features



Fraud prevention best practices



- Partner with third-party providers that can review your security protocols and deliver solutions that shore up any potential points of vulnerability
- Keep your online banking and mobile banking app updated with security patches and require multifactor authentication or biometric data
- Institute alerts and verifications when there is an account-level change
- Flag changes in spending patterns

Q&A Wrap Up

Andy Shank

VP, Fraud and Risk Product Management
Harland Clarke, a Vericast Business

Kellyn Burns

VP, Financial Institutions & Strategic Partnerships
Sontiq

www.harlandclarke.com/webcasts



[harlandclarke.com/LinkedIn](https://www.harlandclarke.com/LinkedIn)



[harlandclarke.com/Twitter](https://www.harlandclarke.com/Twitter)



Type your question in the chat panel 

Thank You