Preventing Fraud at Work

WELCOME

Business Email Compromise

Forms of Business Fraud

Protecting Your Business

Partnering for Prevention

QUESTIONS

Hoosier Hills
CREDIT UNION

Your Presenter: James Aldridge

Hoosier Hills
CREDIT UNION

- CIO for Hoosier Hills Credit Union
- Bachelor's Degree in Information Technology from Ball State
- Master's in Business Administration Degree from University of Indianapolis
- Two-time Mira Award nominee for Tech Innovation and Tech Educator of the Year
- Serves on Computer Technology Advisory Board for Ball State University as well as Business and IT Advisory Board for Vincennes University - Jasper Campus
- Lives in Santa Claus, Indiana

Business Email Compromise

BEC

Red Flags

Find the Red Flags

> Also known as "phishing," business email compromise (BEC) is now the leading tactic for defrauding businesses, recently overtaking Ransomware.
>
> Losses account for $26 billion globally, according to the FBI.

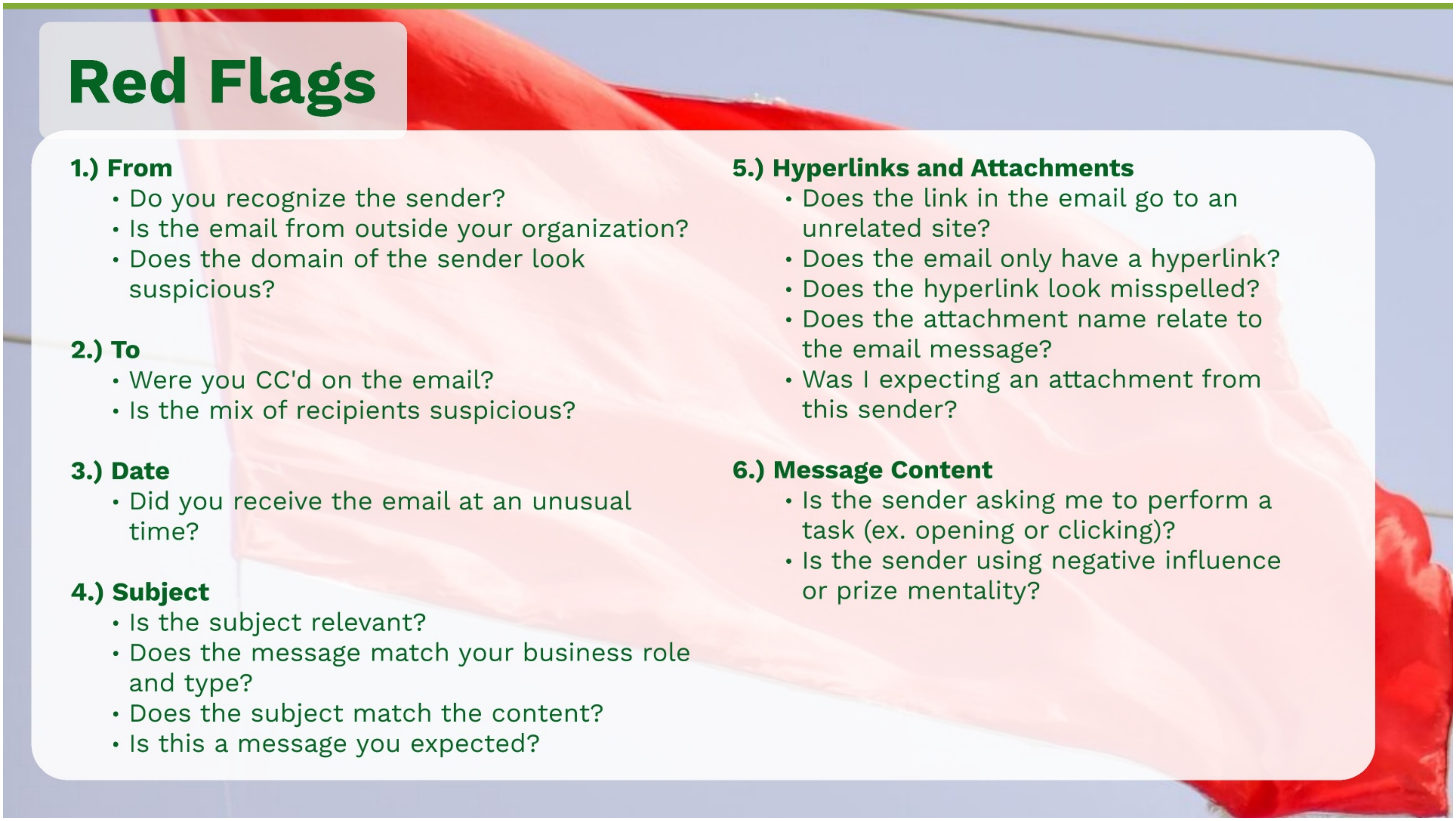
Hoosier Hills
CREDIT UNION

Business Email Compromise

Process:

- Identify target
- Prepare target (Grooming)
- Information exchange
- Goal accomplished (wire or personally identifiable information)
- Flight

Hoosier Hills
CREDIT UNION



Red Flags

1.) From

- Do you recognize the sender?
- Is the email from outside your organization?
- Does the domain of the sender look suspicious?

2.) To

- Were you CC'd on the email?
- Is the mix of recipients suspicious?

3.) Date

- Did you receive the email at an unusual time?

4.) Subject

- Is the subject relevant?
- Does the message match your business role and type?
- Does the subject match the content?
- Is this a message you expected?

5.) Hyperlinks and Attachments

- Does the link in the email go to an unrelated site?
- Does the email only have a hyperlink?
- Does the hyperlink look misspelled?
- Does the attachment name relate to the email message?
- Was I expecting an attachment from this sender?

6.) Message Content

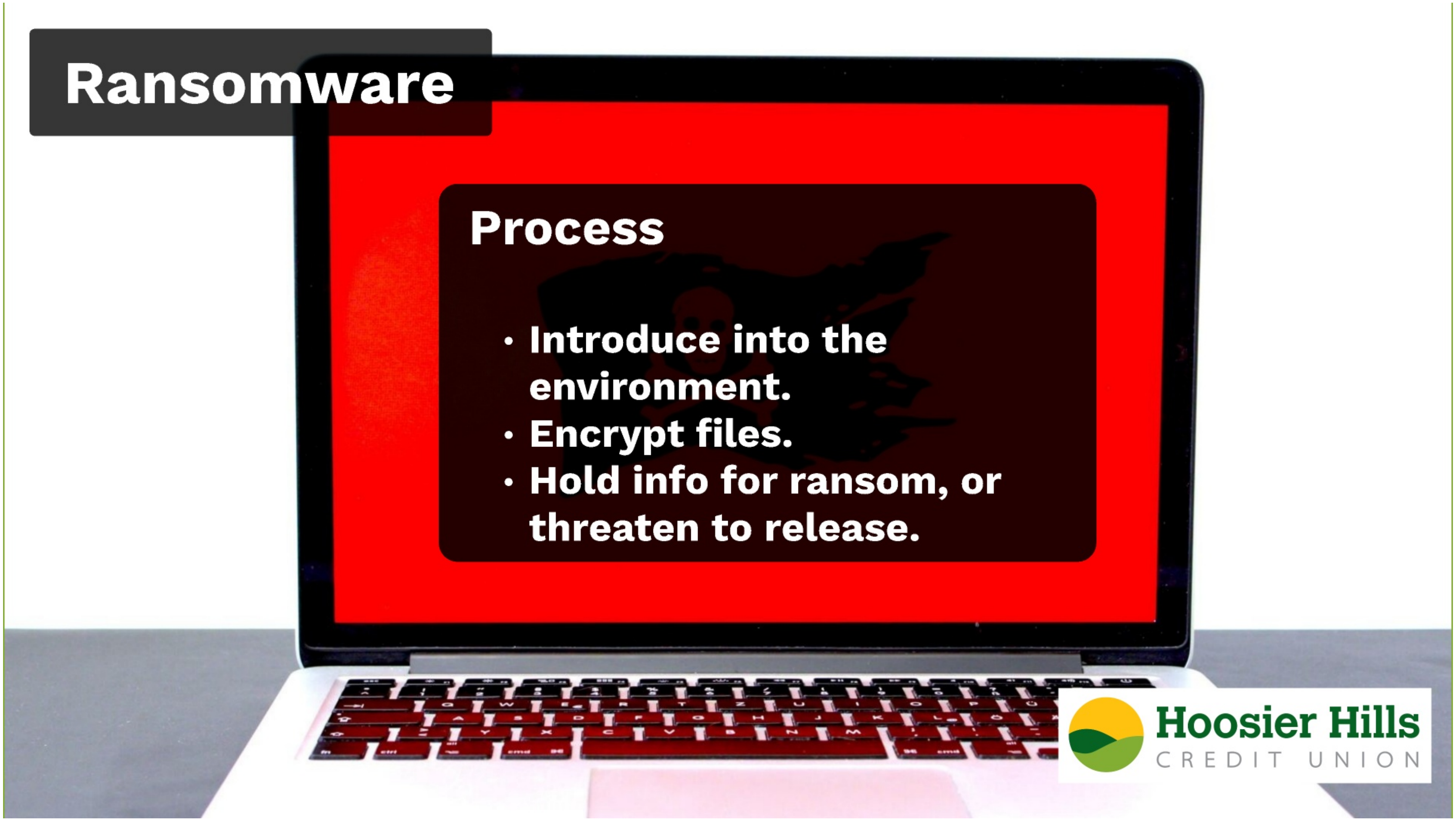
- Is the sender asking me to perform a task (ex. opening or clicking)?
- Is the sender using negative influence or prize mentality?

Other Common Forms of Business-Related Fraud

- Ransomware
- Vishing
- Physical Threats

Hoosier Hills
CREDIT UNION

Ransomware



Process

- Introduce into the environment.
- Encrypt files.
- Hold info for ransom, or threaten to release.

Hoosier Hills
CREDIT UNION

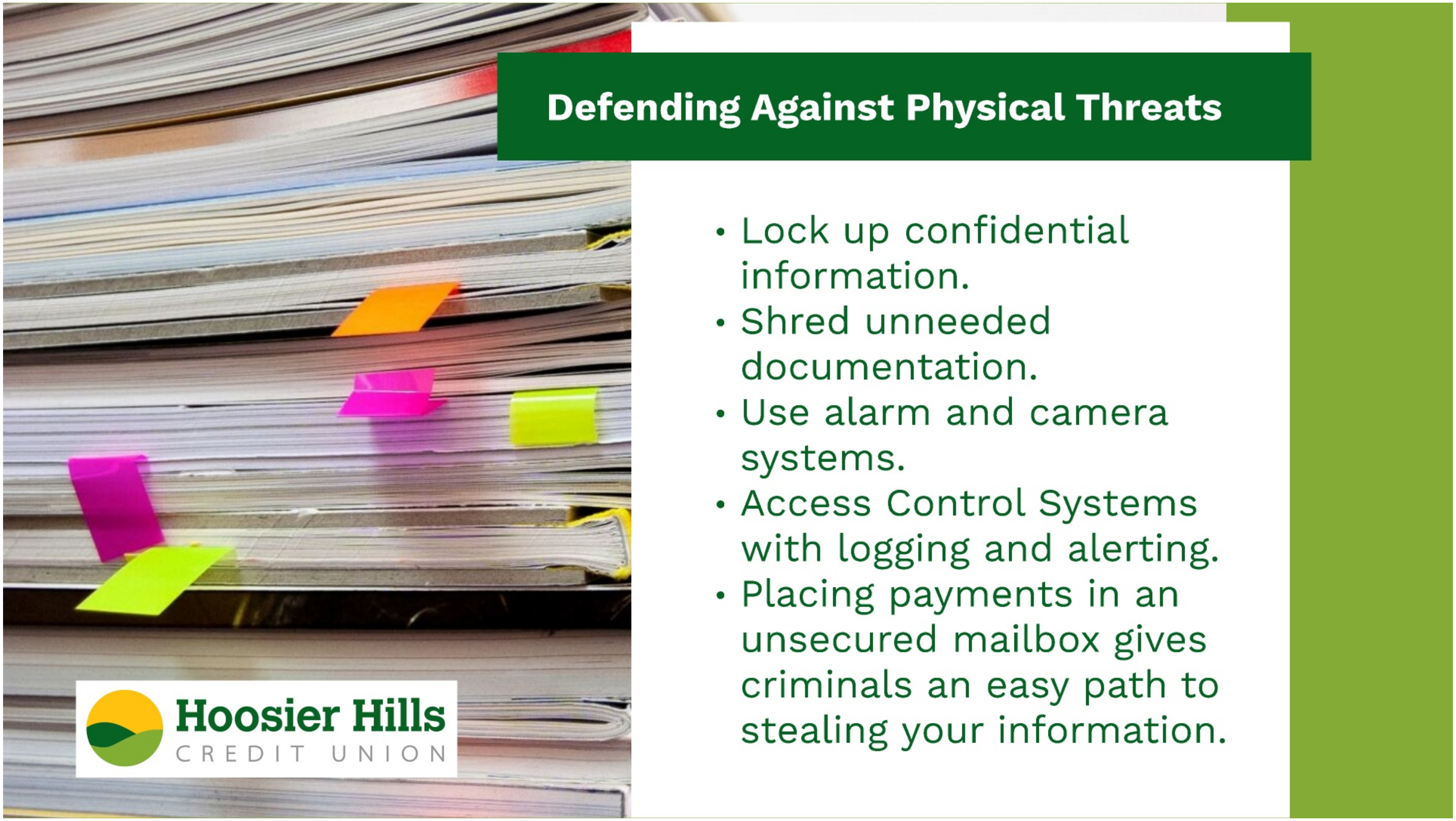
Vishing

Limit sharing employer and schedule information.

Vishing is the same scam as phishing/ BEC using voice. They want the same information and they use the same tactics to rush and confuse their victims.

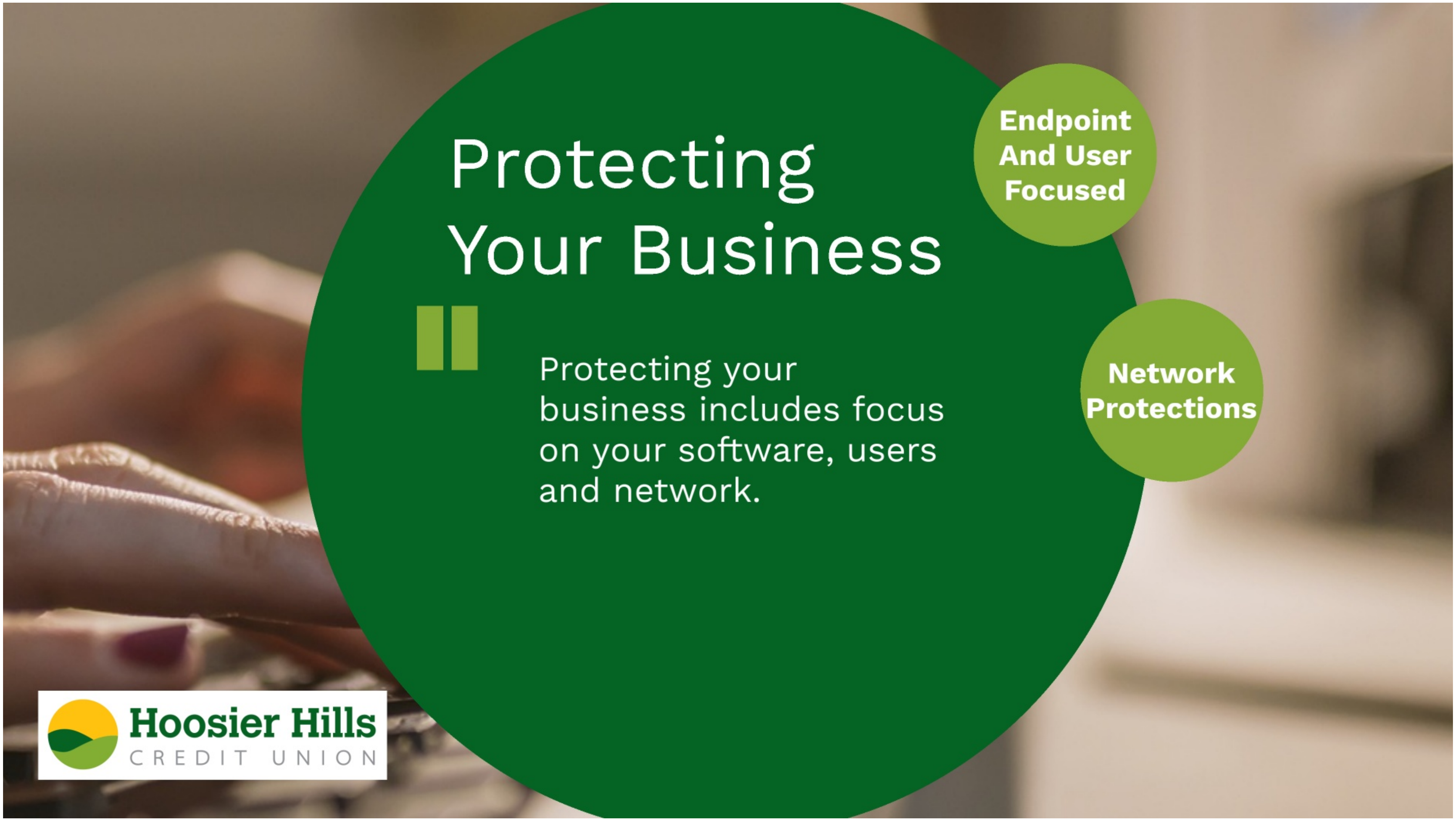
Criminals can use **spoofing** to make their phone number appear to come from someone else, including your FI.

Hoosier Hills
CREDIT UNION


Hoosier Hills
CREDIT UNION

Defending Against Physical Threats

- Lock up confidential information.
- Shred unneeded documentation.
- Use alarm and camera systems.
- Access Control Systems with logging and alerting.
- Placing payments in an unsecured mailbox gives criminals an easy path to stealing your information.



Protecting Your Business

"

Protecting your business includes focus on your software, users and network.

Endpoint And User Focused

Network Protections

Hoosier Hills CREDIT UNION

Endpoint and User Focused

- End user education
- Endpoint protection: antivirus, anti malware
- Endpoint encryption
- Endpoint firewalls

Basic Network Protections

- Disable old or unused email, applications and domain accounts.
- Use multifactor authentication.
- Have a data backup plan.
- Maintain hardware/software asset inventory.
- Utilize firewall (malware protection, content filtering, whitelist, blacklist, geoblocking, command and control callbacks, IDS/IPS.

Partner in Fraud Prevention

> Keeping your accounts protected is a top priority for both HHCU and the members we serve.

HHCU

Members

What to Do

Hoosier Hills
CREDIT UNION

HHCU: Here to Protect Your Business

Wire Request Verification

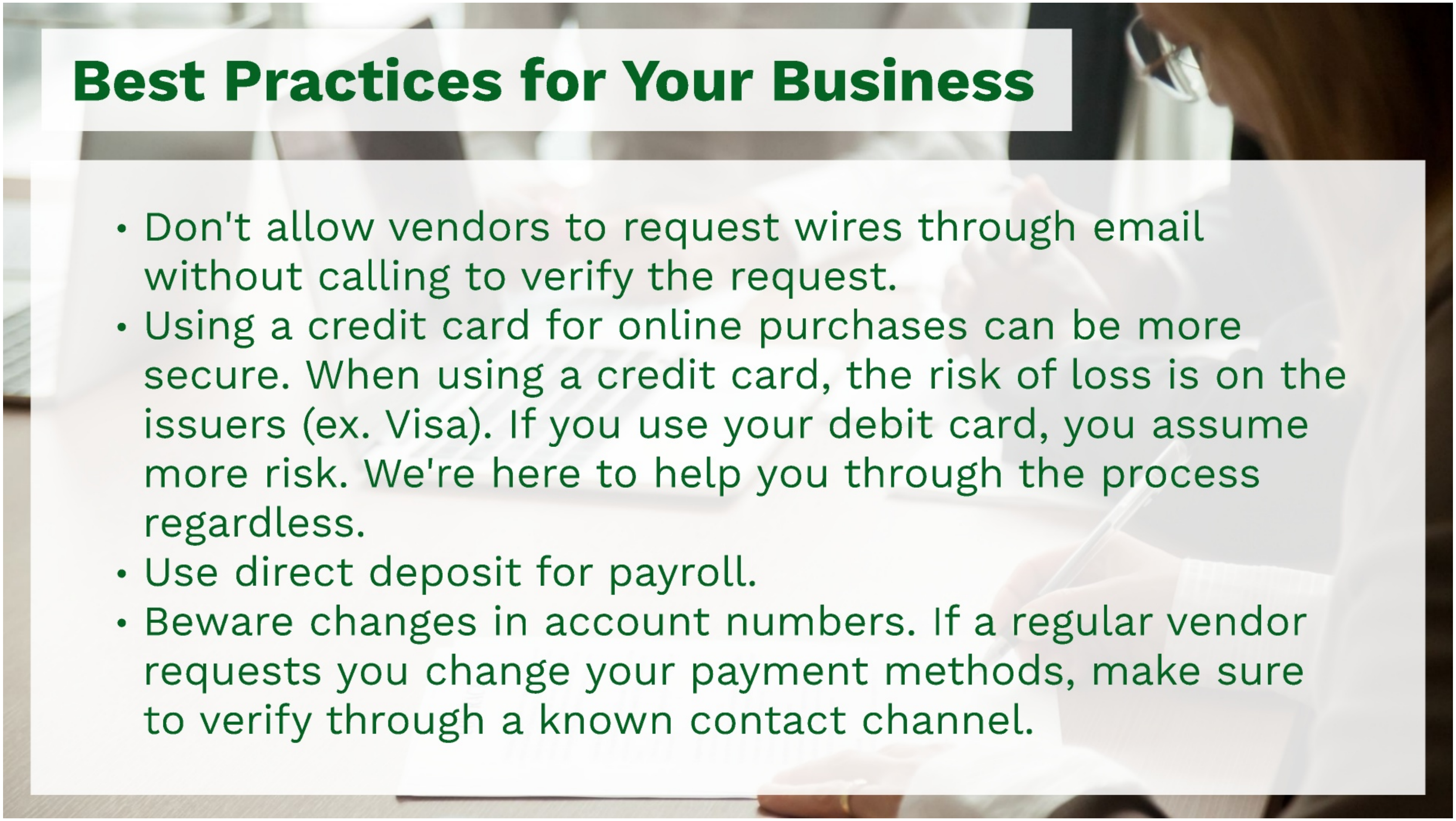
Before we complete wire transactions, we'll contact you to confirm the request. Once wires are sent to fraudulent accounts, recovery can be difficult or even impossible.

Geographic Restrictions

To keep your accounts secure, we place geographic restrictions on out of state and country debit charges.

CardValet

Turn cards on and off from your phone. Set geographic and merchant type limits by card and employee.



Best Practices for Your Business

- Don't allow vendors to request wires through email without calling to verify the request.
- Using a credit card for online purchases can be more secure. When using a credit card, the risk of loss is on the issuers (ex. Visa). If you use your debit card, you assume more risk. We're here to help you through the process regardless.
- Use direct deposit for payroll.
- Beware changes in account numbers. If a regular vendor requests you change your payment methods, make sure to verify through a known contact channel.

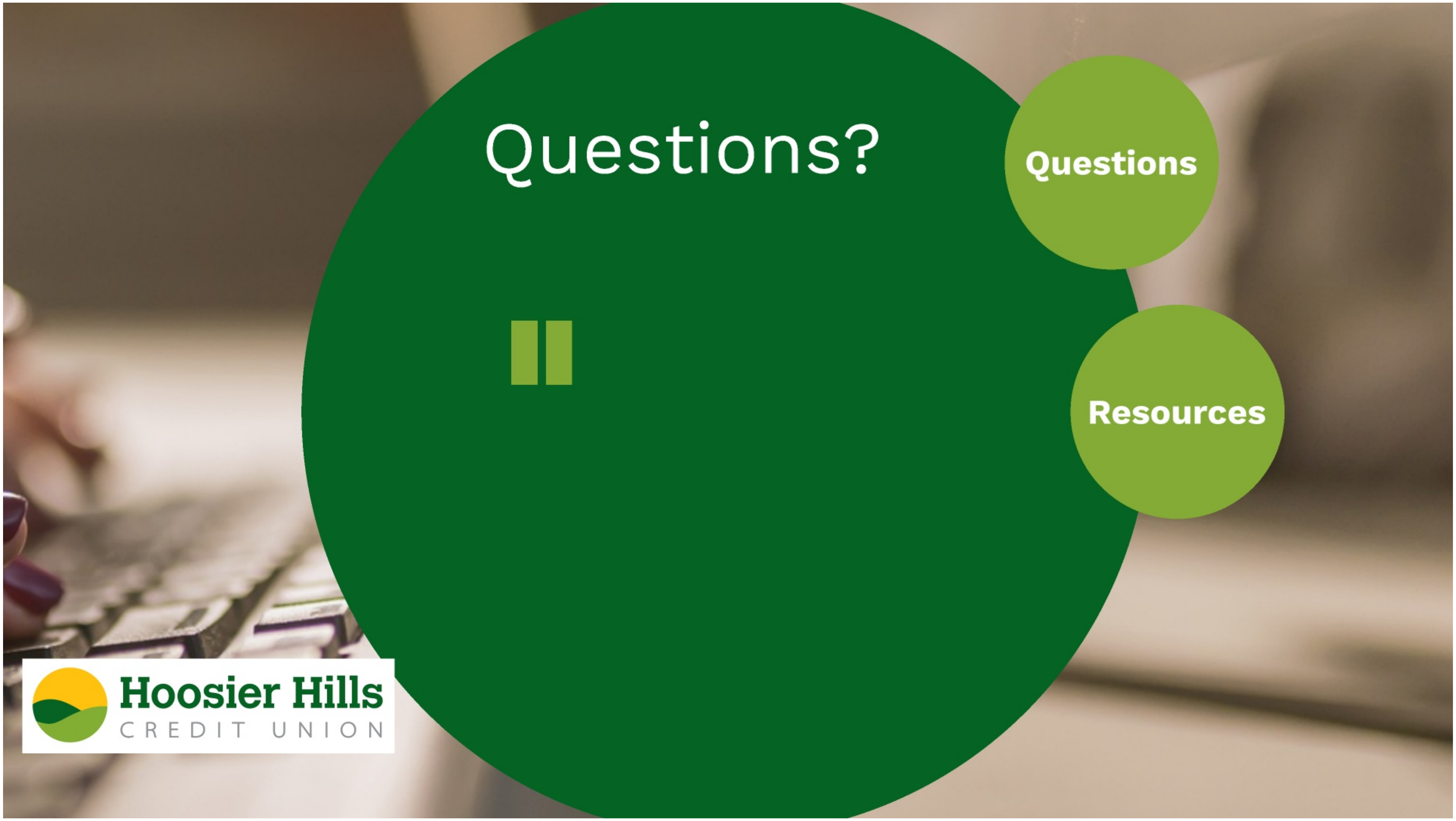
What To Do If You Suspect Fraud

Call us at 800.865.2612, or visit your nearest Service Center.

To report a misused card after hours call 800.472.3272.

Use CardValet to immediately turn cards on and off.

Initiate Dispute Tracking in Online or Mobile Banking.



Questions?

Questions

Resources

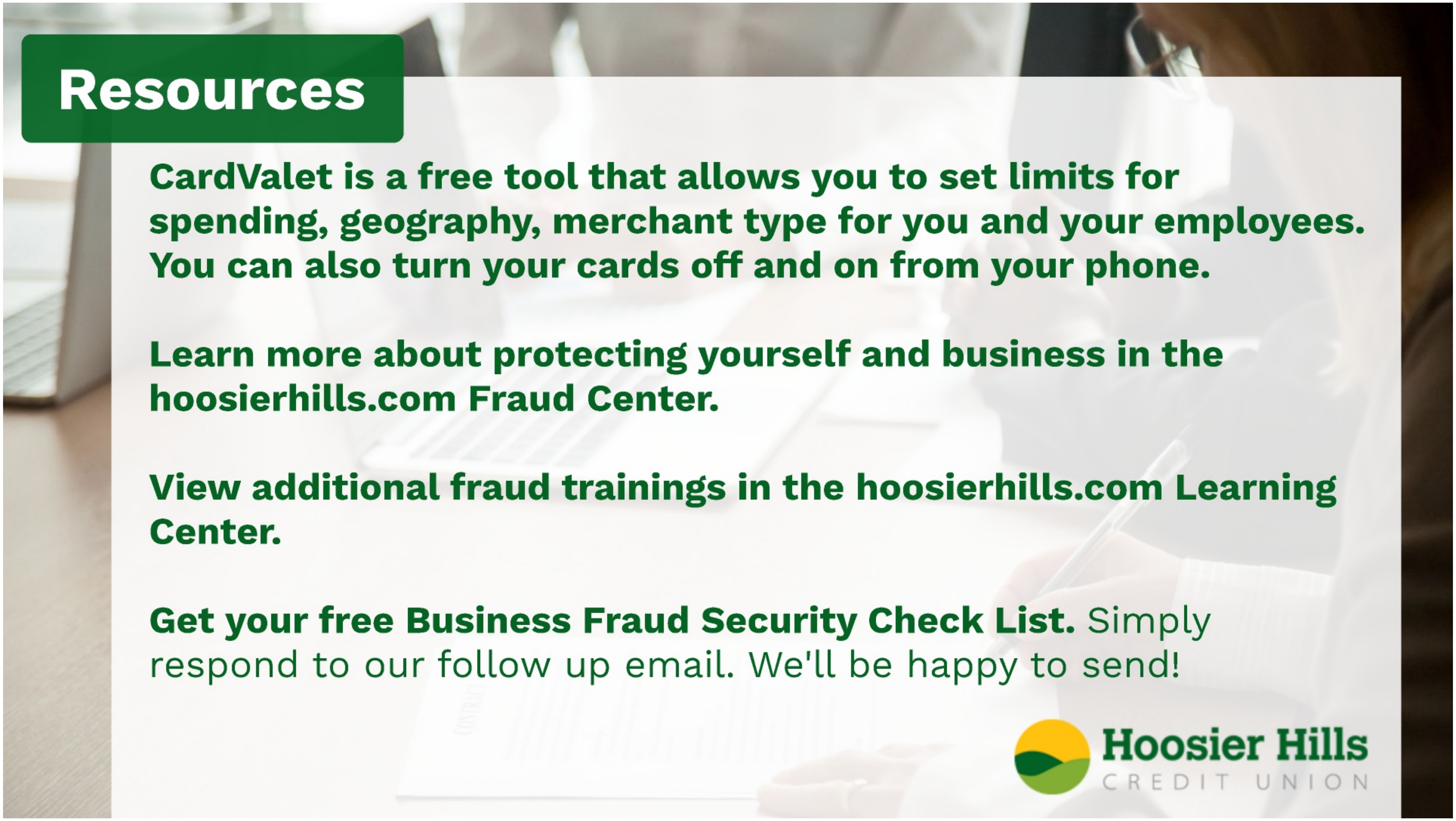
Hoosier Hills
CREDIT UNION

Questions

Can you provide more information on NIST and CIS 20?

How do you recommend we get started with security awareness training?

Is it worth getting a security consultant to assist us with developing an IT security strategy?



Resources

CardValet is a free tool that allows you to set limits for spending, geography, merchant type for you and your employees. You can also turn your cards off and on from your phone.

Learn more about protecting yourself and business in the hoosierhills.com Fraud Center.

View additional fraud trainings in the hoosierhills.com Learning Center.

Get your free Business Fraud Security Check List. Simply respond to our follow up email. We'll be happy to send!

Hoosier Hills
CREDIT UNION