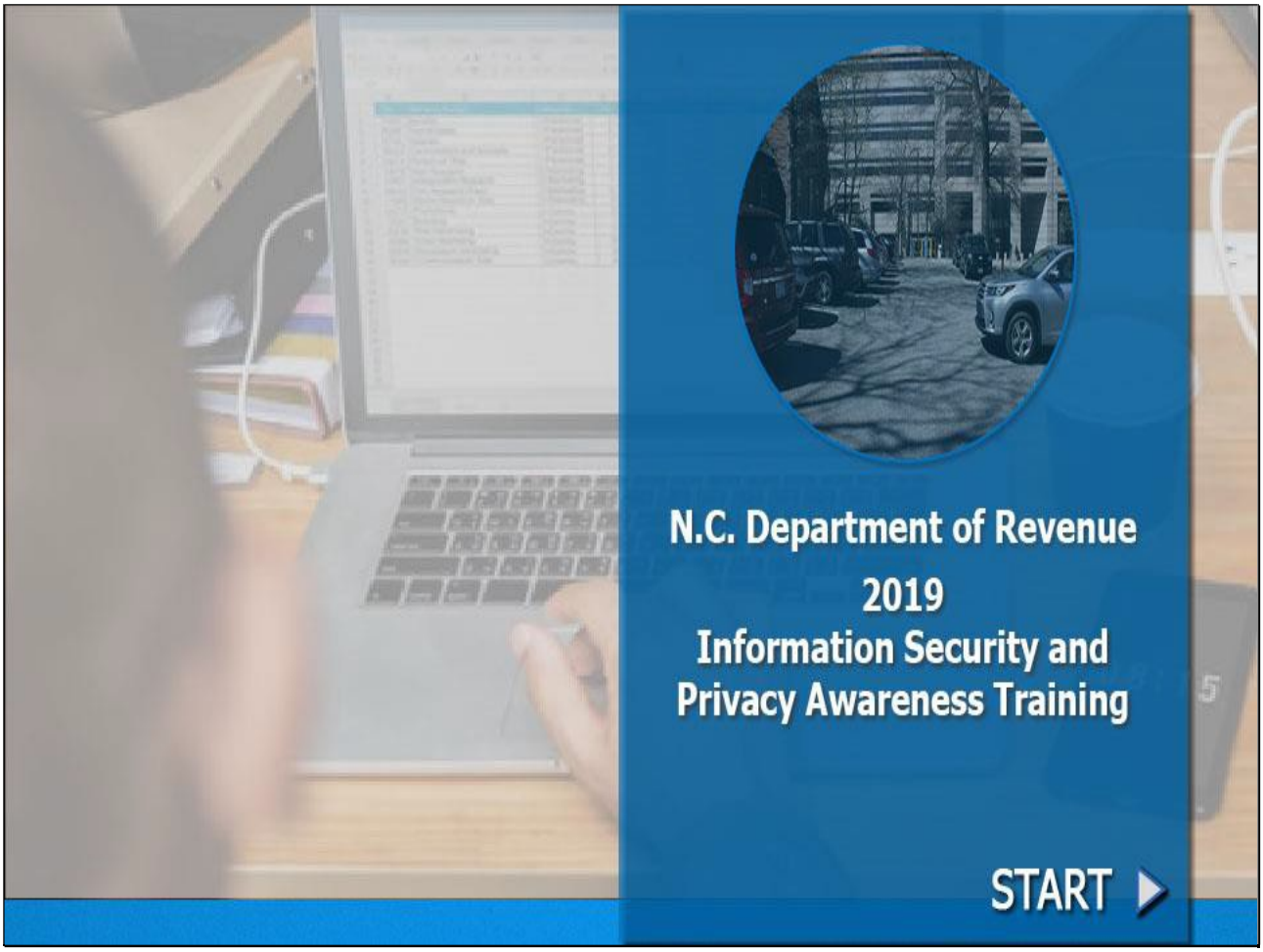
2019 Information Security and Privacy Awareness Training



Notes

Welcome to the 2019 North Carolina Department of Revenue's Information Security and Privacy Awareness Training.

The importance of Information Security and Privacy

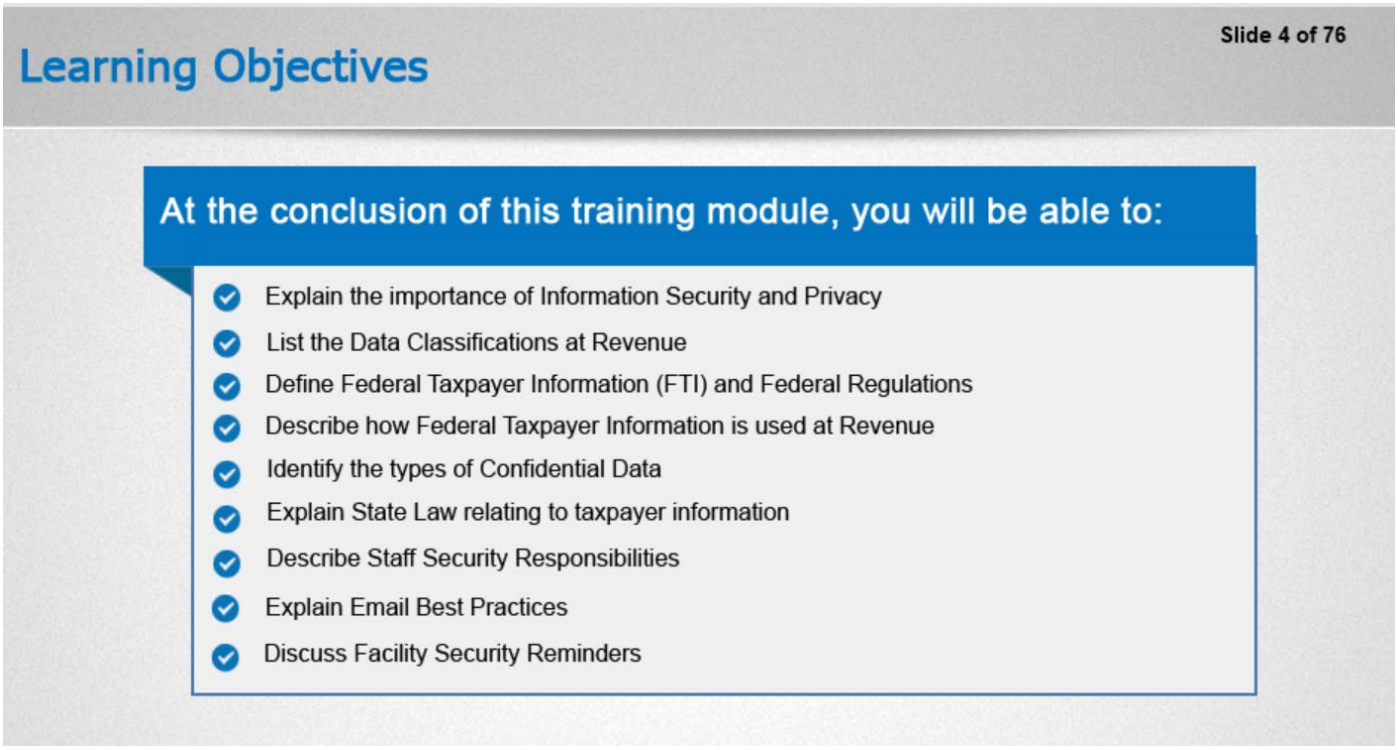
Video Transcript

Information Security is extremely important for the Department of Revenue for several reasons. One reason is State law requires us to protect all the information that we have.

The second is we have a special relationship with the IRS so we also receive federal data. Federal law requires that we protect all the information.

I think the primary reason it is important is that the citizens of North Carolina have entrusted us with very sensitive information and there's an expectation from them that we protect their information.

Learning Objectives

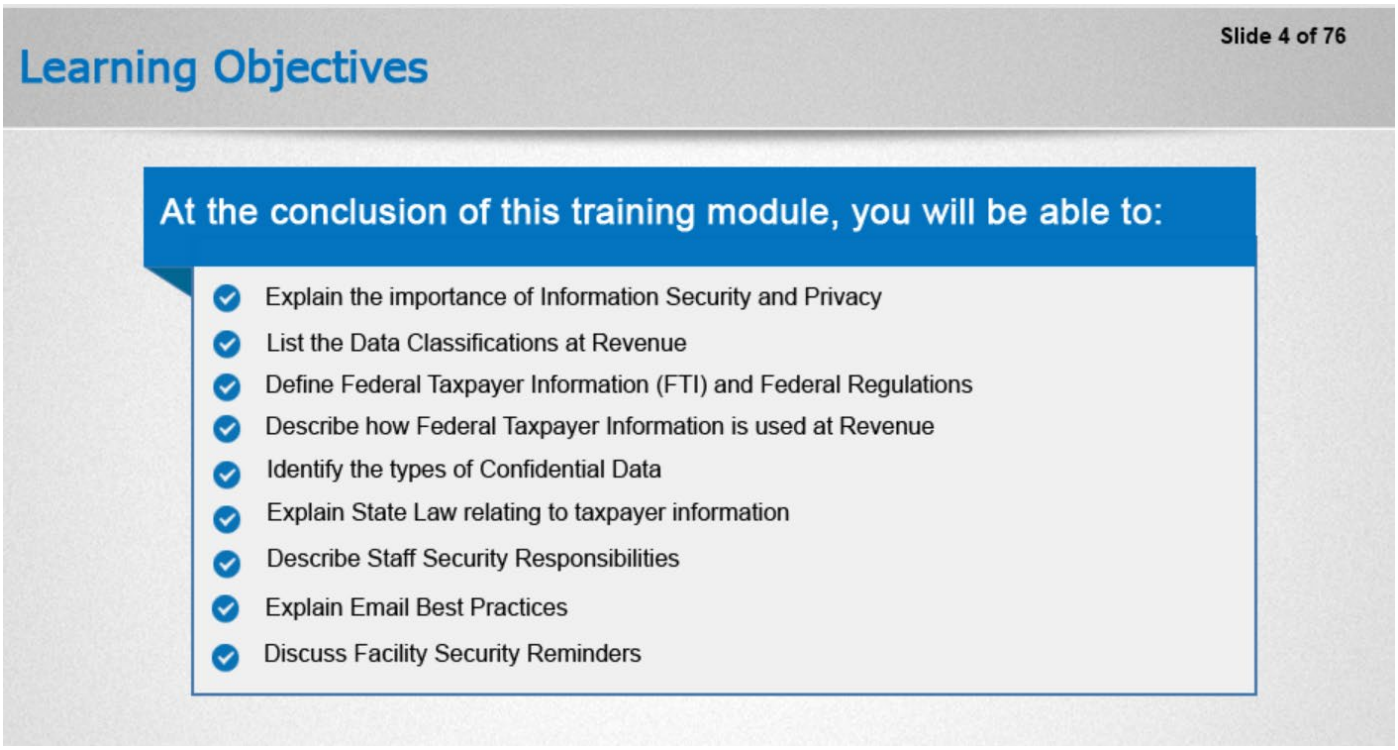


Notes

At the conclusion of this training module, you will be able to:

- Explain the importance of Information Security and Privacy
- List the Data Classifications at Revenue
- Define Federal Taxpayer Information (FTI) and Federal Regulations
- Describe how Federal Taxpayer Information is used at Revenue
- Identify types of Confidential Data
- Explain State Law relating to taxpayer information

Learning Objectives, cont.



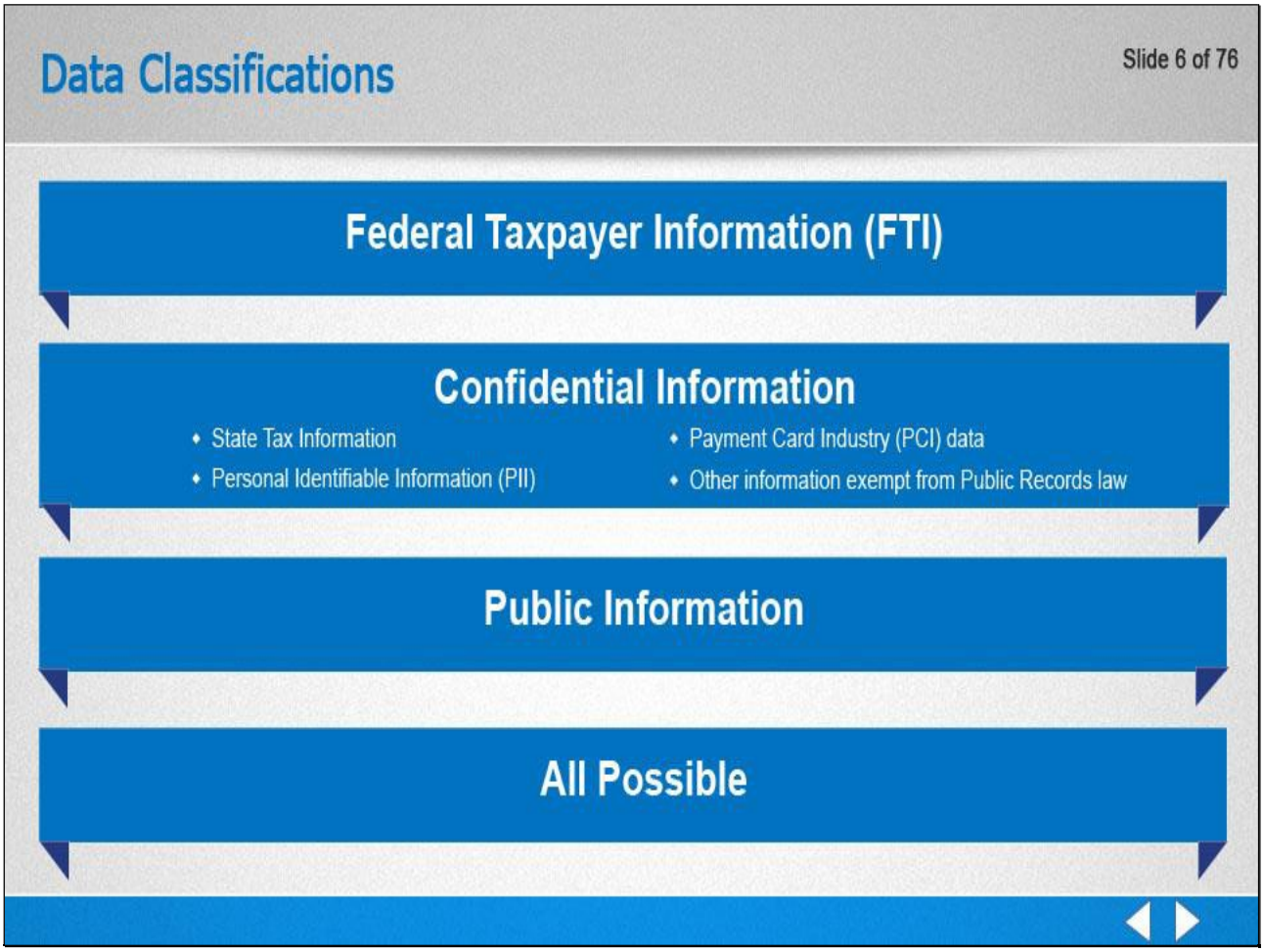
Notes, cont.

- Describe Staff Security Responsibilities
- Explain Email Best Practices
- Discuss Facility Security Reminders

Important Terms

Key Terms	Definitions
Resources	Broadly interpreted to refer to any computing device such as a server, pc, smart phone, tablet or any other such device that can process or transmit information digitally.
Data	Electronic information in any form, regardless of source, that is created or obtained by the Agency.
Staff	Anyone working on behalf of the Agency regardless of employment status and includes contractual relationships for entities that provide goods or services.

Data Classifications



Notes

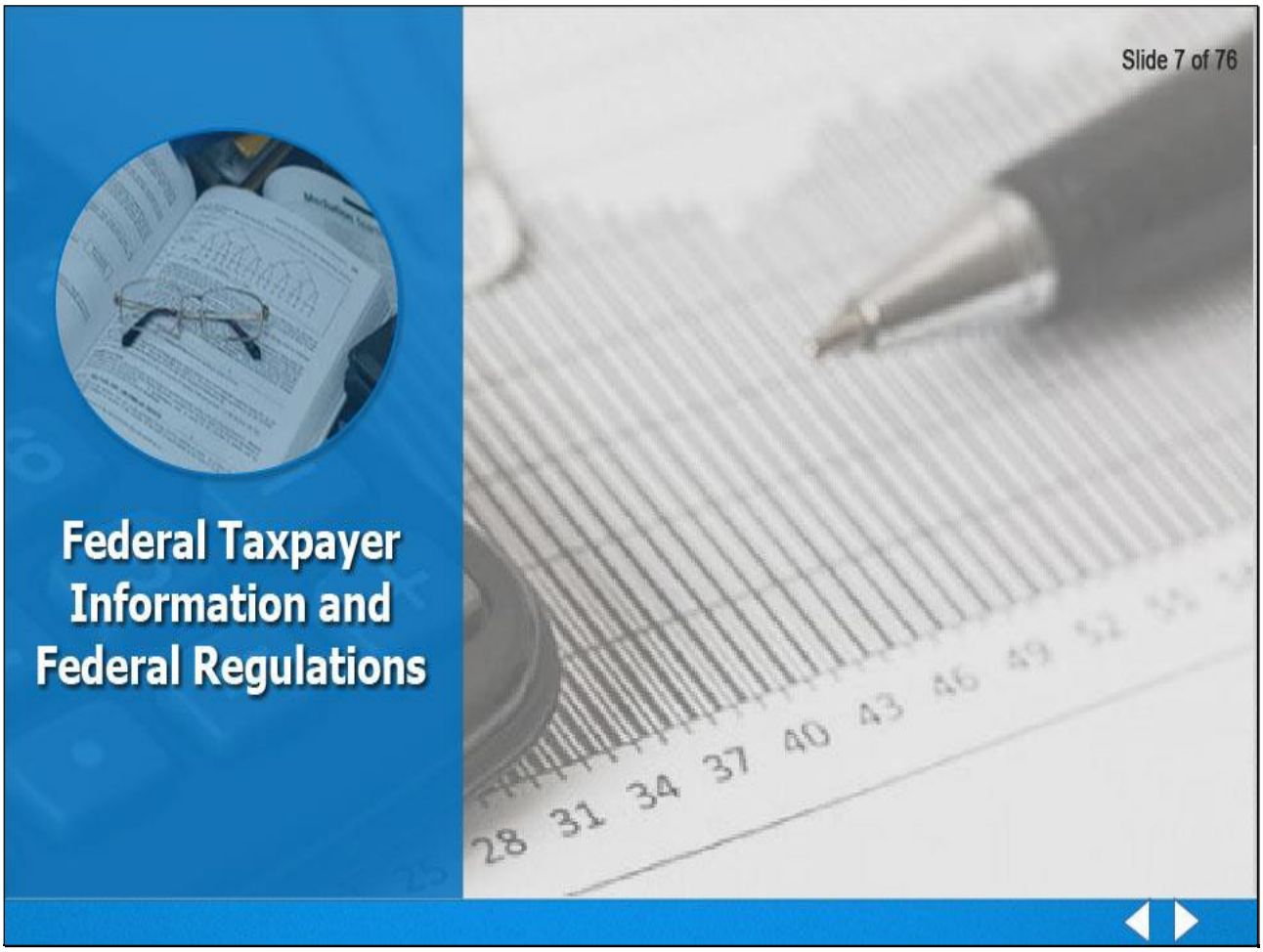
There are four data classifications used at Revenue. They are:

- Federal Taxpayer Information
- Confidential Information
- Public Information, and
- All Possible.

We will discuss each of these within this training module, including the different types of confidential information that you may encounter while working at DOR.

Federal Taxpayer Information and Confidential Information should be protected and handled with care.

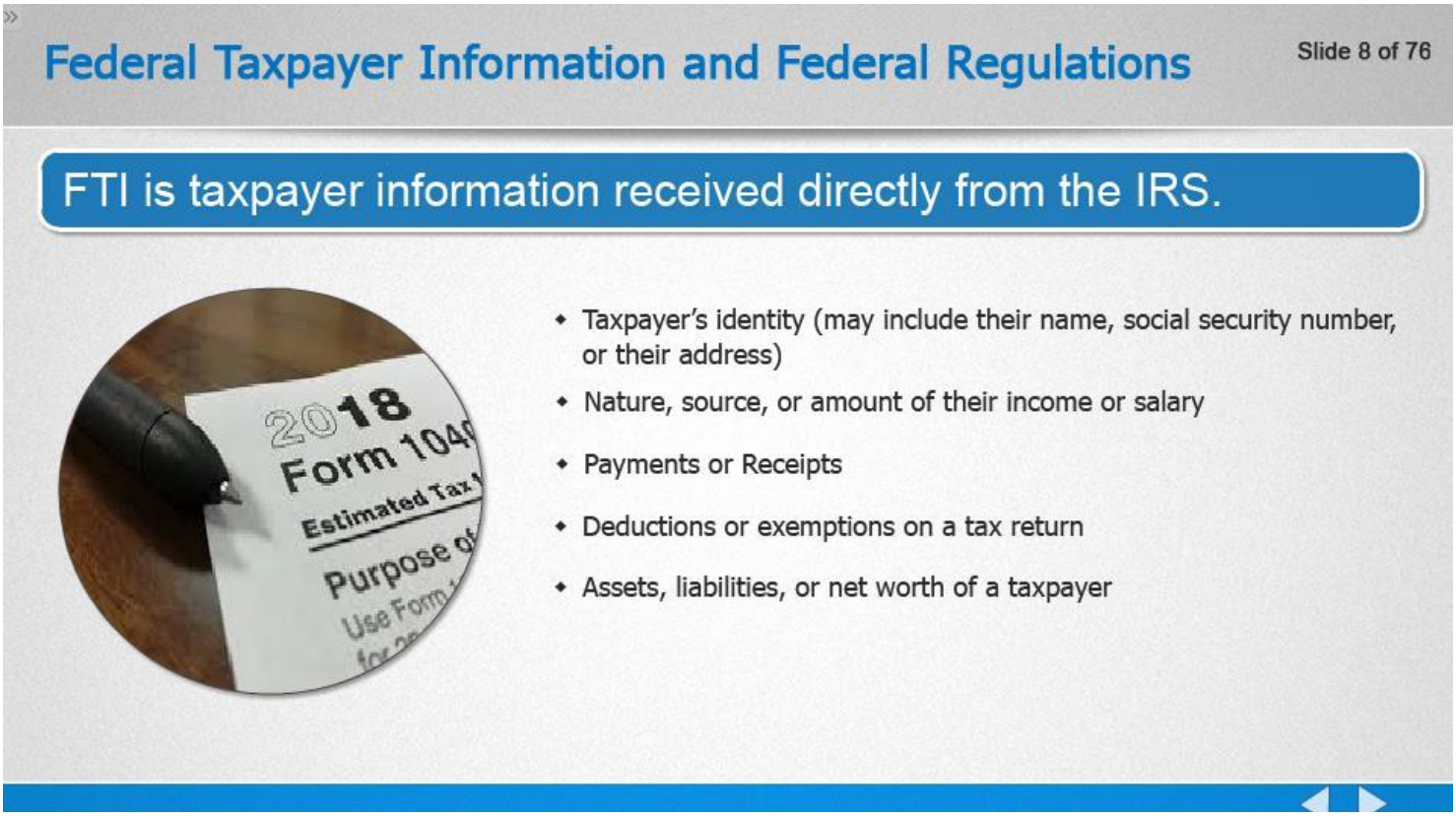
Federal Taxpayer Information and Federal Regulations



Notes

Now let’s discuss Federal Taxpayer Information and Federal Regulations that are required at Revenue.

FTI and Federal Regulations



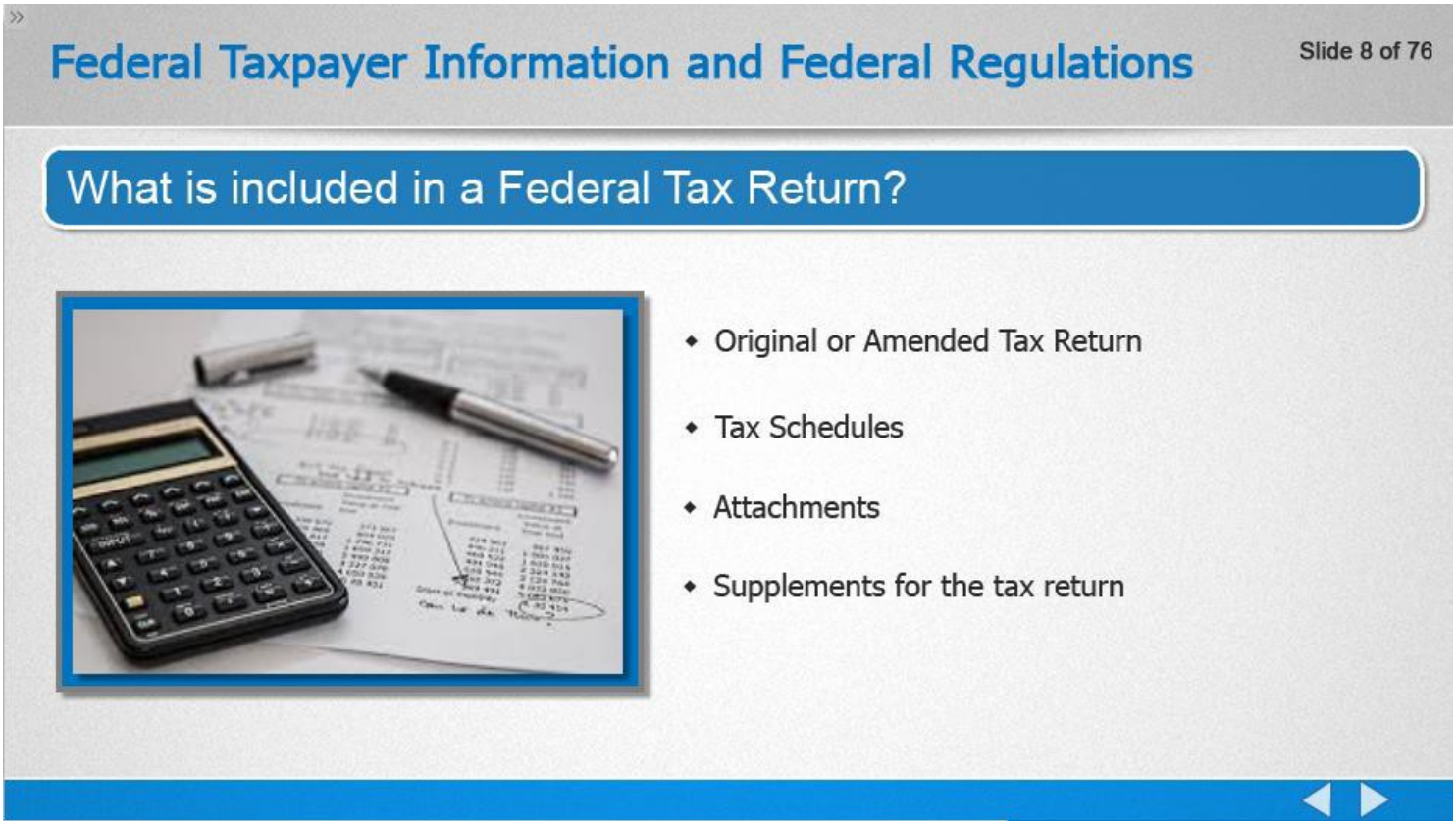
Notes

What is Federal Taxpayer Information or FTI?

Federal Taxpayer information is taxpayer information that is received directly from the IRS, and it may include the following:

- Any information that would identify a taxpayer. This may include their name, social security number, or their address
- The nature, source, or amount of their income or salary
- Payments or receipts
- Deductions or exemptions on a tax return, and
- The assets, liabilities, or net worth of a taxpayer

FTI and Federal Regulations, cont.



Notes, cont.

You might wonder what is included in a Federal Tax Return.

Well, a return may include the following:

- Original and amended tax returns
- Tax schedules
- Attachments, and
- Supplements for the tax return

FTI and Federal Regulations, cont.

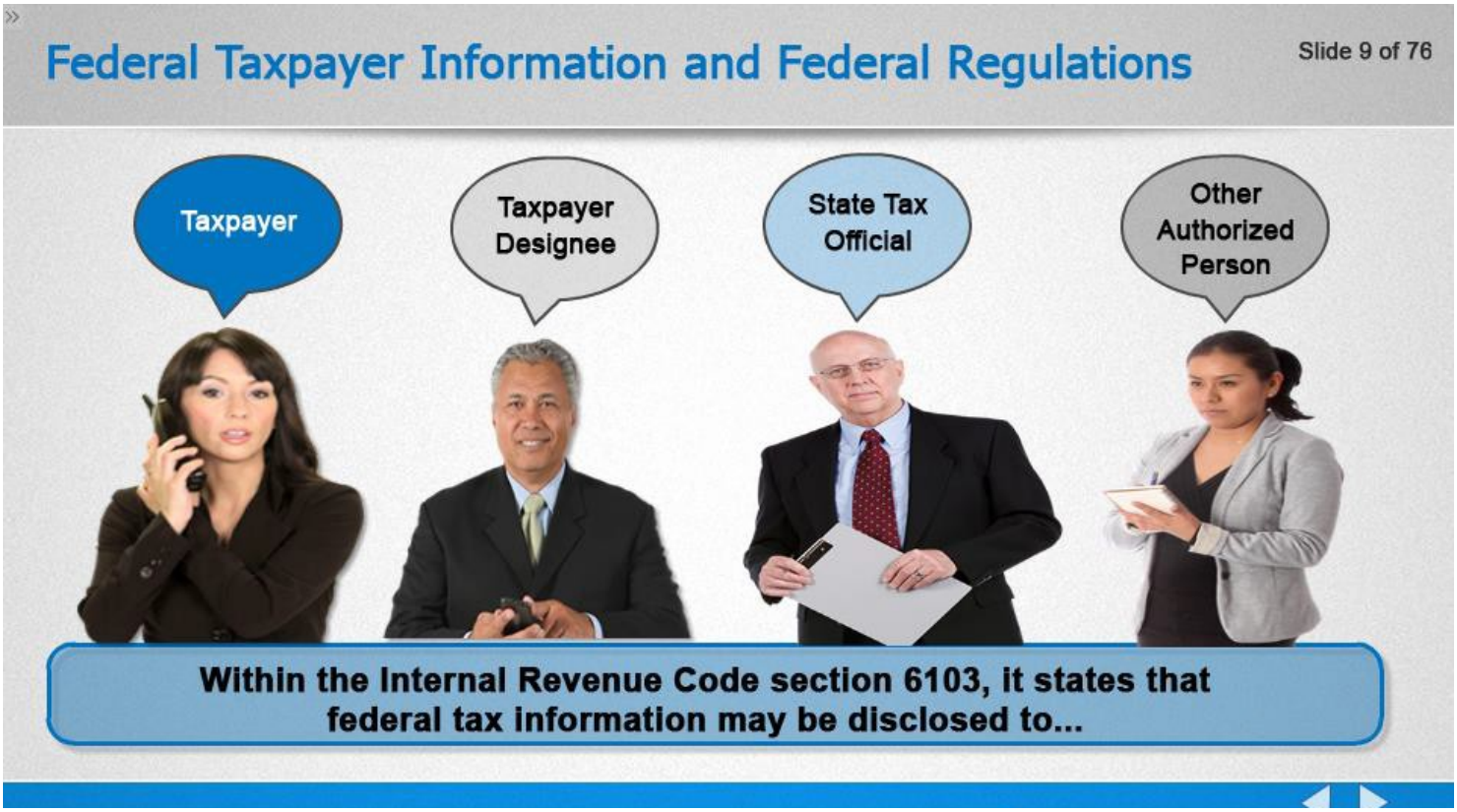
Notes, cont.

FTI can also include business tax schedules such as:

- Corporate (including S Corp)
- Partnership
- Withholding, and
- Excise

It is important to note that the DOR receives information for audit results on these schedules.

FTI and Federal Regulations



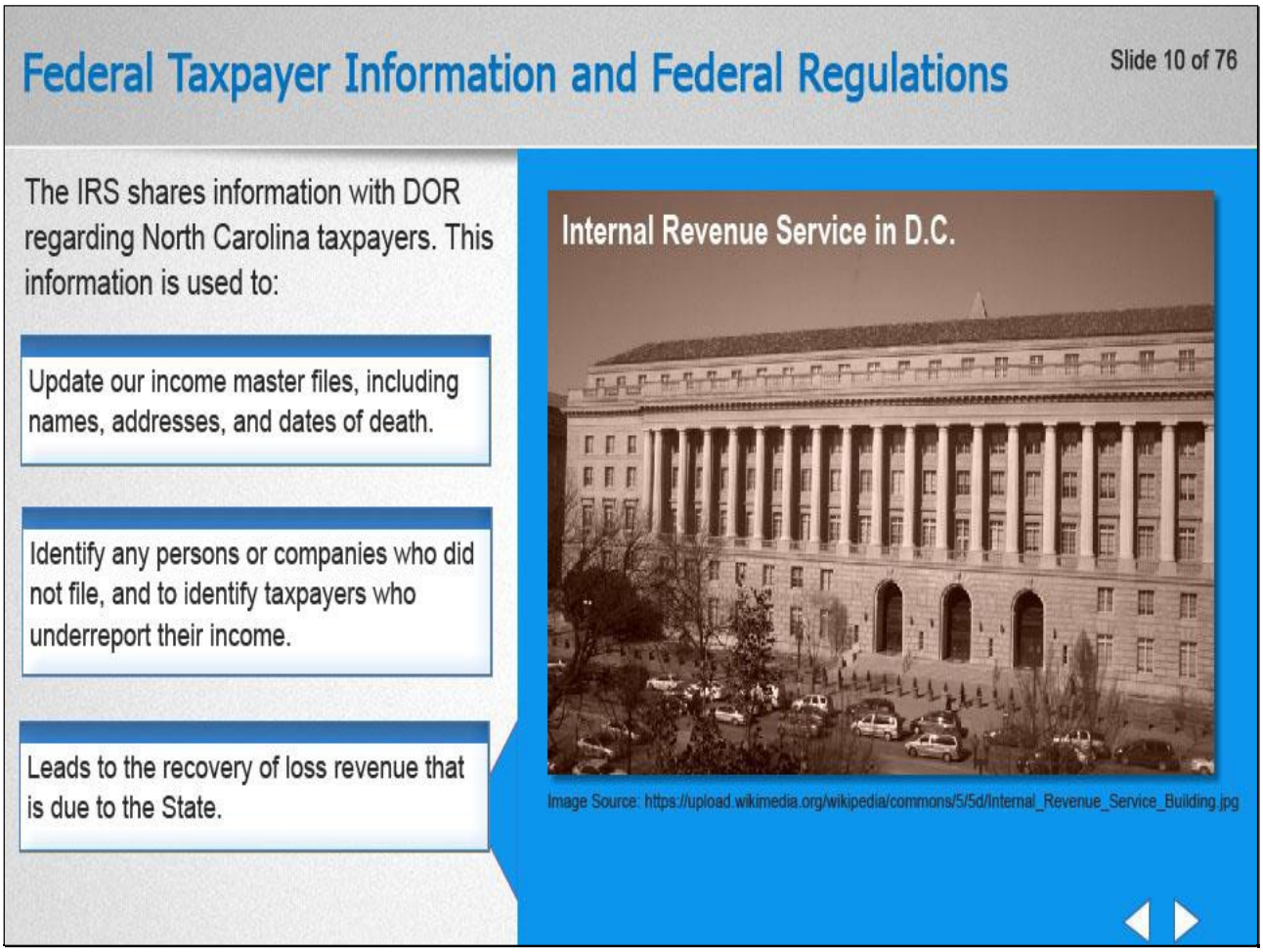
Notes

Within the Internal Revenue Code section 6103, it states that Federal Tax Information may be disclosed to:

- The actual taxpayer of the tax return and return information
- The taxpayer's designee provided a Power of Attorney has been provided for this person from the taxpayer.
- State Tax Officials including Revenue staff with a business need to use information for tax administration purposes.
- Other persons who are authorized and with a need to know.

If you have questions regarding who you are able to disclose tax information to, please contact your NCDOR supervisor.

Federal Taxpayer Information and Federal Regulations



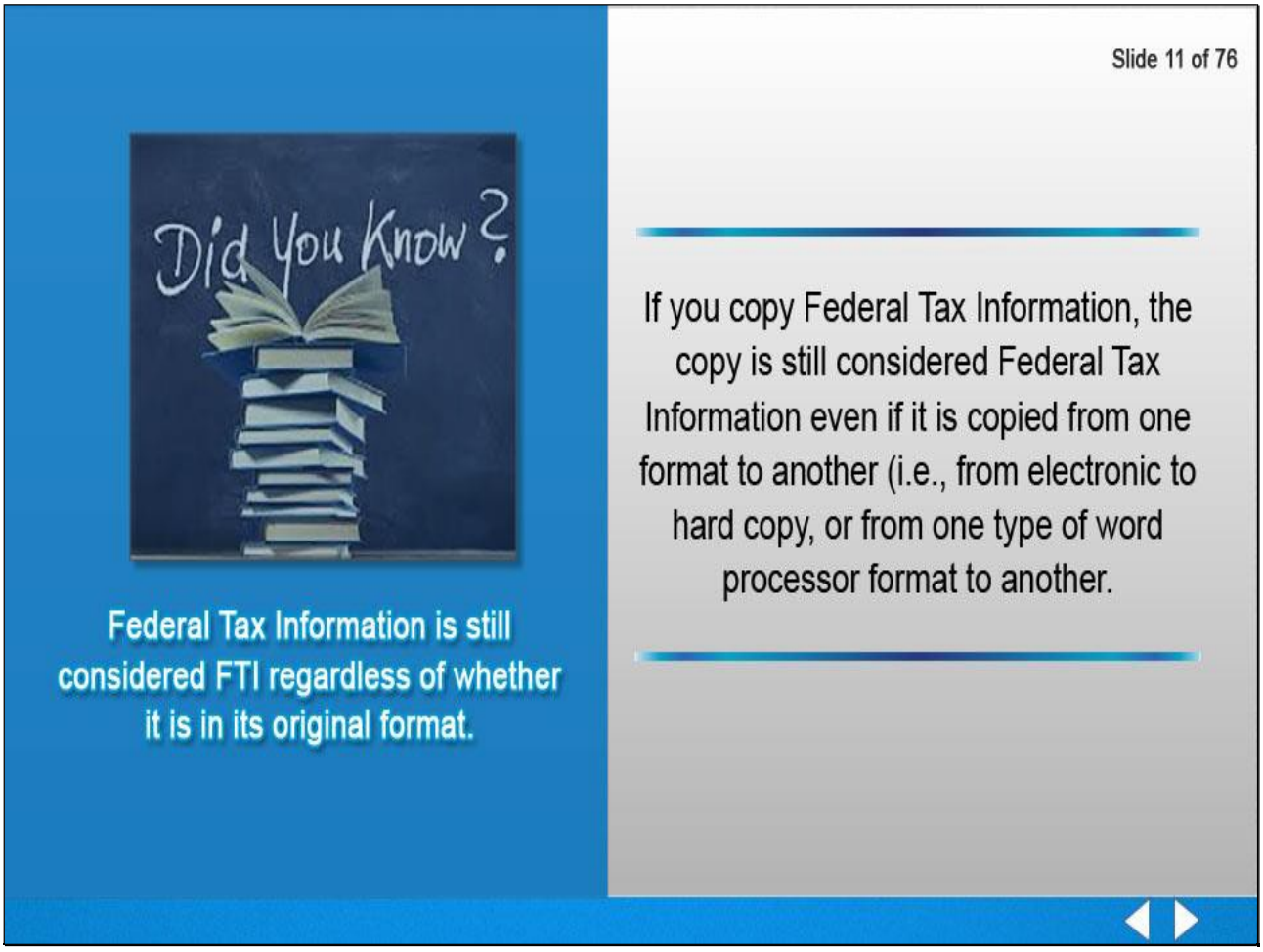
Notes

Working together, the Internal Revenue Service and Revenue share information regarding North Carolina taxpayers.

Revenue uses this information to:

- Update our income tax master files, including taxpayer names, addresses, and dates of death.
- Identify any persons or companies who did not file referred to as non-filing taxpayers) for North Carolina and to identify taxpayers who underreport their income.
- All of this helps our agency recover lost revenue due to our State.

Did You Know?



Notes

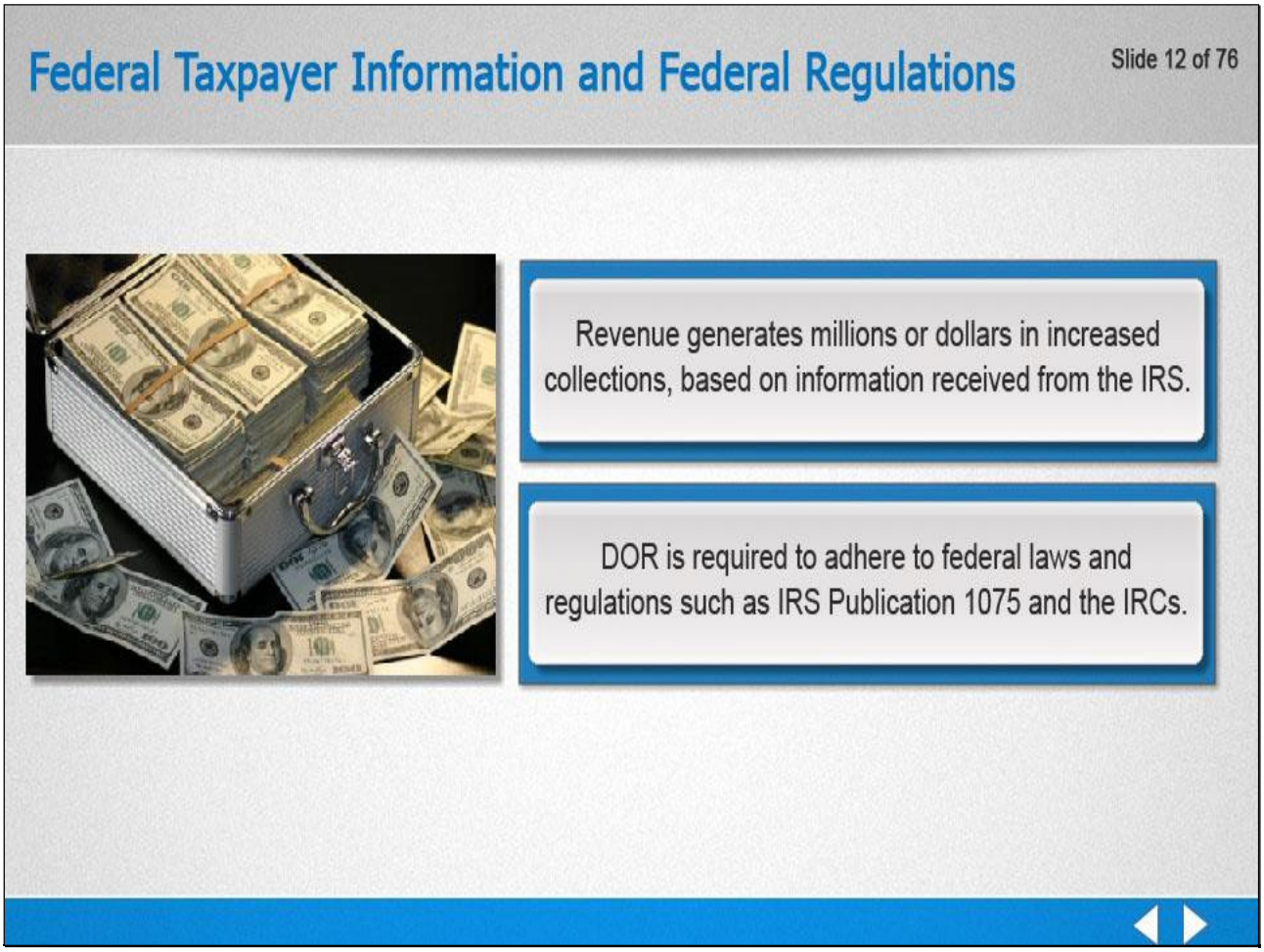
Did You Know, if you copy federal tax information at all, even from one format to another, it is still considered federal tax information.

For example, if a NCDOR staff member generates a report that contains

FTI through the use of an application on his/her workstation and then prints out the report, the printed report is also classified as FTI. All copies have the same handling requirements as the original document.

Remembering this concept will ensure that all FTI is tracked and logged accordingly per IRS requirement.

FTI and Federal Regulations



Notes

During an average fiscal year, Revenue generates millions of dollars in increased collections based on information received from the Internal Revenue Service. So, you can see how valuable this information is to our agency.

Since most of the income surplus our agency has goes back to the state legislature, who in turn distributes it to other state agencies via budget allocations, it helps the entire state. In order to keep receiving information from the Internal Revenue Service, we are required to adhere to federal laws and regulations.

These include the Internal Revenue Service Publication 1075, and the Internal Revenue Code sections that are covered later in this training.

What is Commingling?

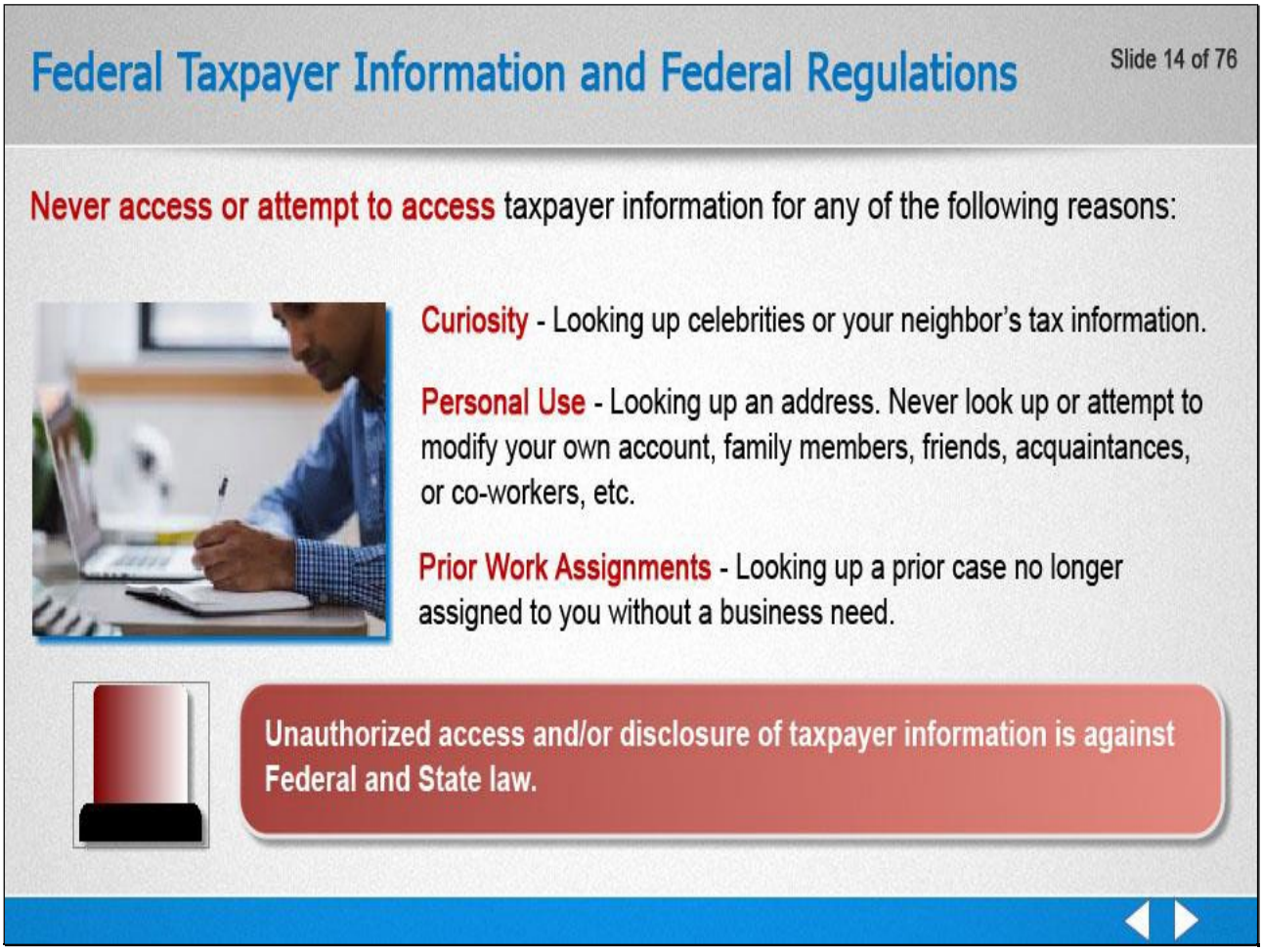
Notes

When FTI is combined with State tax information, it is referred to as Commingled data.

Commingling of Federal and State tax information subjects the entire file to the safeguard requirements mandated by the IRS.

Commingled data must be protected as required by the federal law from unauthorized access, disclosure, and inspection.

FTI and Federal Regulations

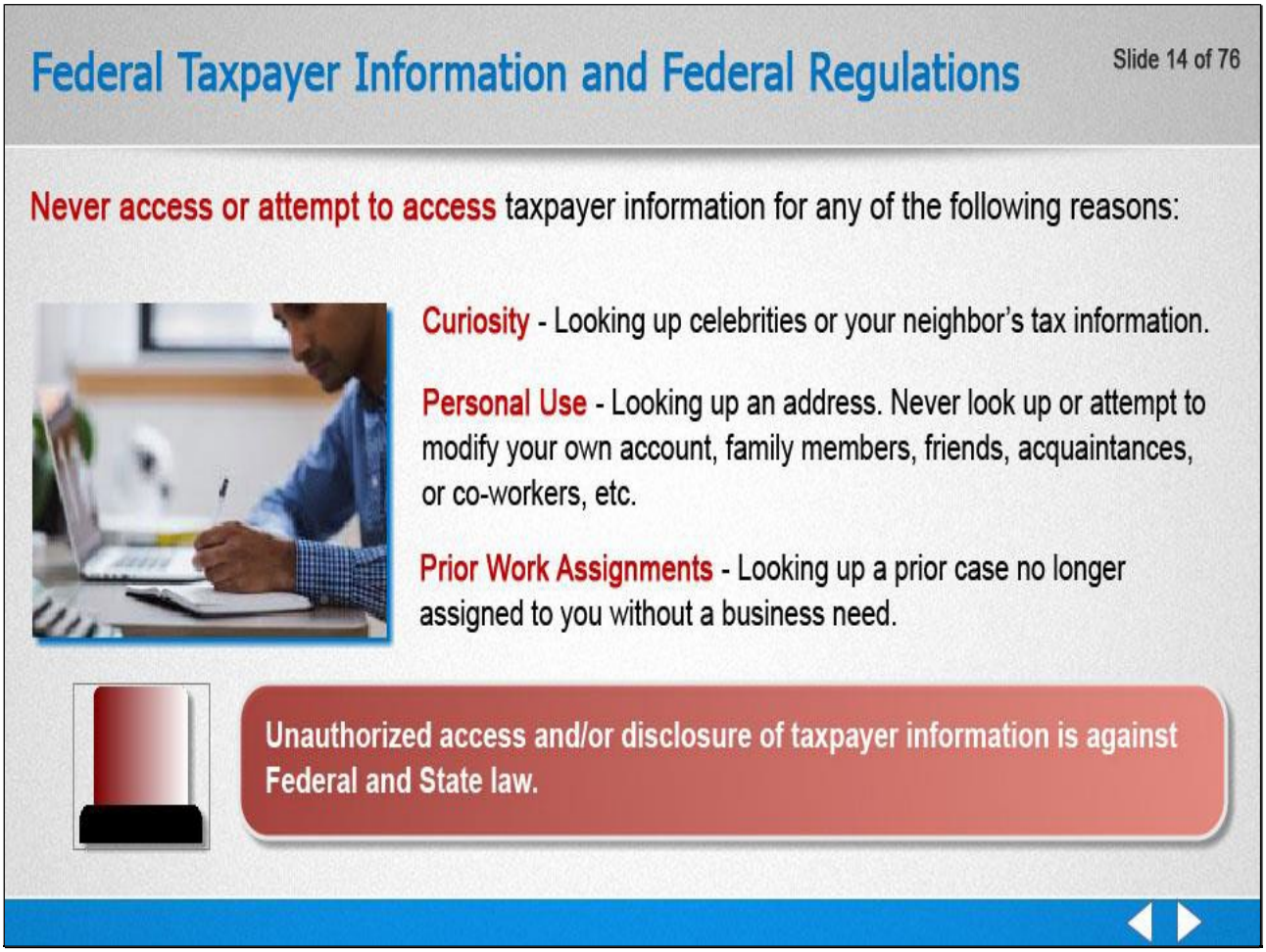


Notes

To protect FTI or commingled data, you should never access or attempt to access taxpayer information for any of the following reasons:

- To satisfy a curiosity such as looking up celebrities or your neighbor's tax information
- For personal use such as looking up a taxpayer's address. You should never look up or attempt to modify account information for yourself, a family member, friends, acquaintances, co-workers, or anyone else without a business need,
- Or to check on prior work assignments. By looking up a prior case that is no longer assigned to you is considered accessing it without a business need.

FTI and Federal Regulations, cont.



Notes, cont.

If you are assigned an audit or you receive tax information for someone that you have a personal relationship with or know on a person level as part of your job assignments, you should notify your supervisor immediately.

Remember, all systems at Revenue are monitored. Unauthorized access and/or disclosure of taxpayer information is against Federal and State law.

Links to IRS Training Videos

Protecting Federal Tax Information: A Message from the IRS
https://www.irsvideos.gov/Governments/Safeguards/ProtectingTaxInformation

Safeguards Security Awareness Training
https://www.irsvideos.gov/Governments/Safeguards/SafeguardsSecurityAwarenessTraining

Confidential Data

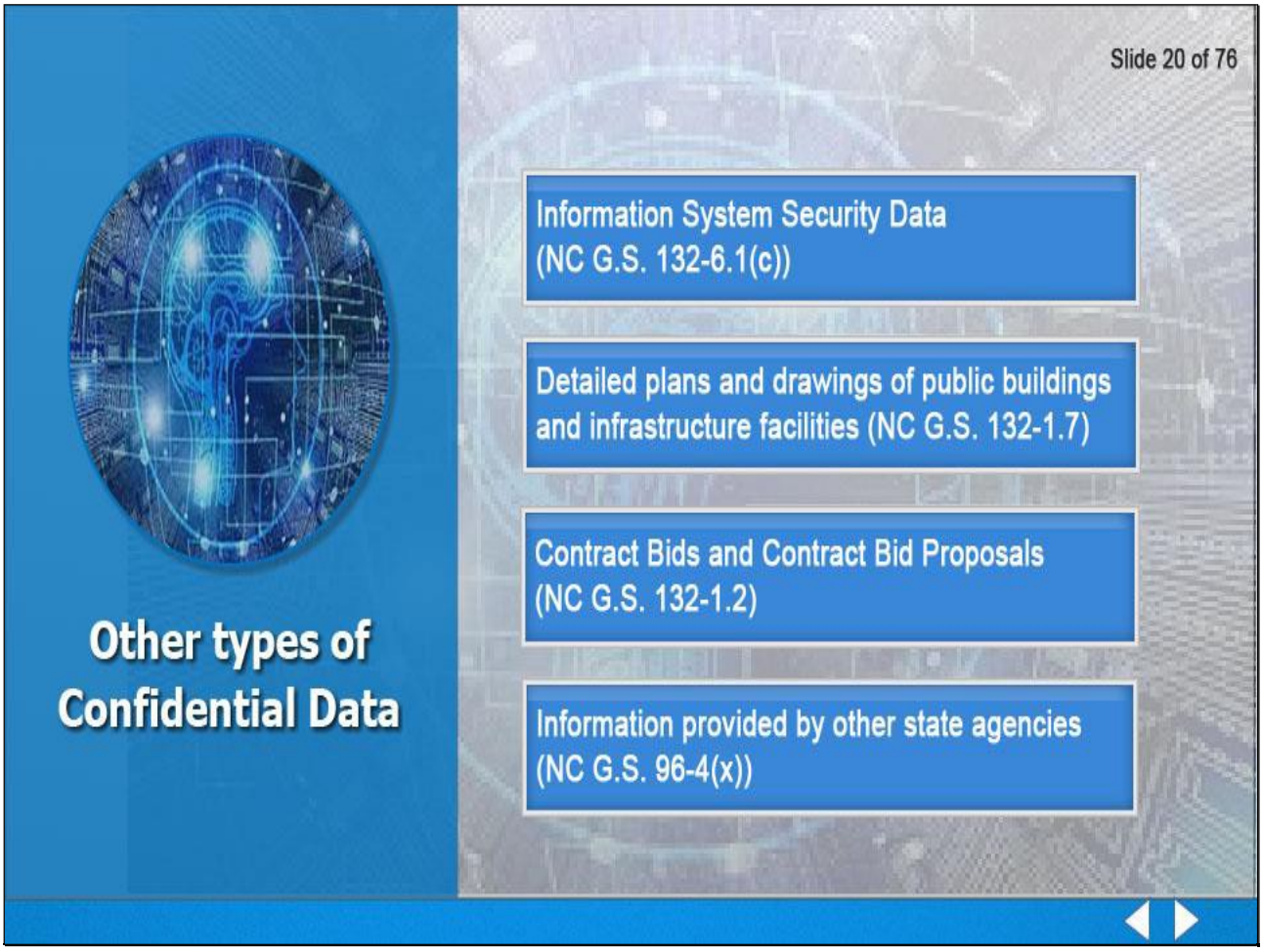
Notes

Now that we have defined Federal Taxpayer Information and Federal Regulations let's identify the different types of confidential data that we must protect. Confidential data requires protection and proper destruction. It is important to understand what types of data are considered as confidential.

Confidential data includes:

- Personal Identifiable information is also referred to as Personally Identifiable Information.
- Merchant Credit Card Data
- State Taxpayer Information, and
- User Passwords

Confidential Data, cont.



Notes, cont.

Other types of confidential data include but are not limited to:

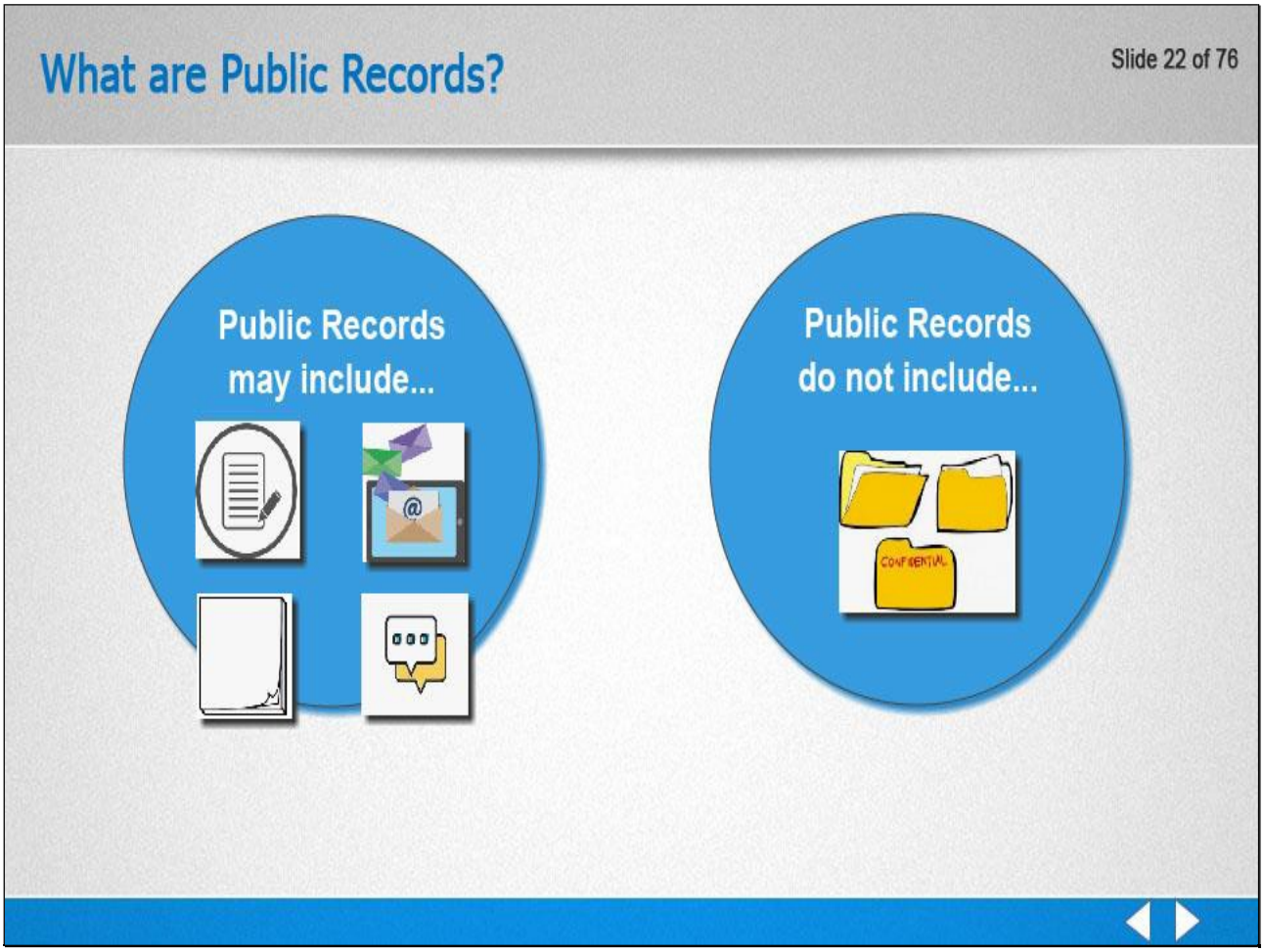
- Information System Security Data which includes data such as security configuration settings and other data about the security of our systems.
- Detailed plans and drawings of public buildings and infrastructure facilities
- Contract Bids and Contract Bid Proposals that include identified vendor trade secrets and Information provided by other state agencies for tax administration purposes.

State Laws and Taxpayer Information

Notes

Now that we have identified the types of confidential data that we protect at Revenue, let's discuss State Laws and Taxpayer Information.

What are Public Records?



Notes

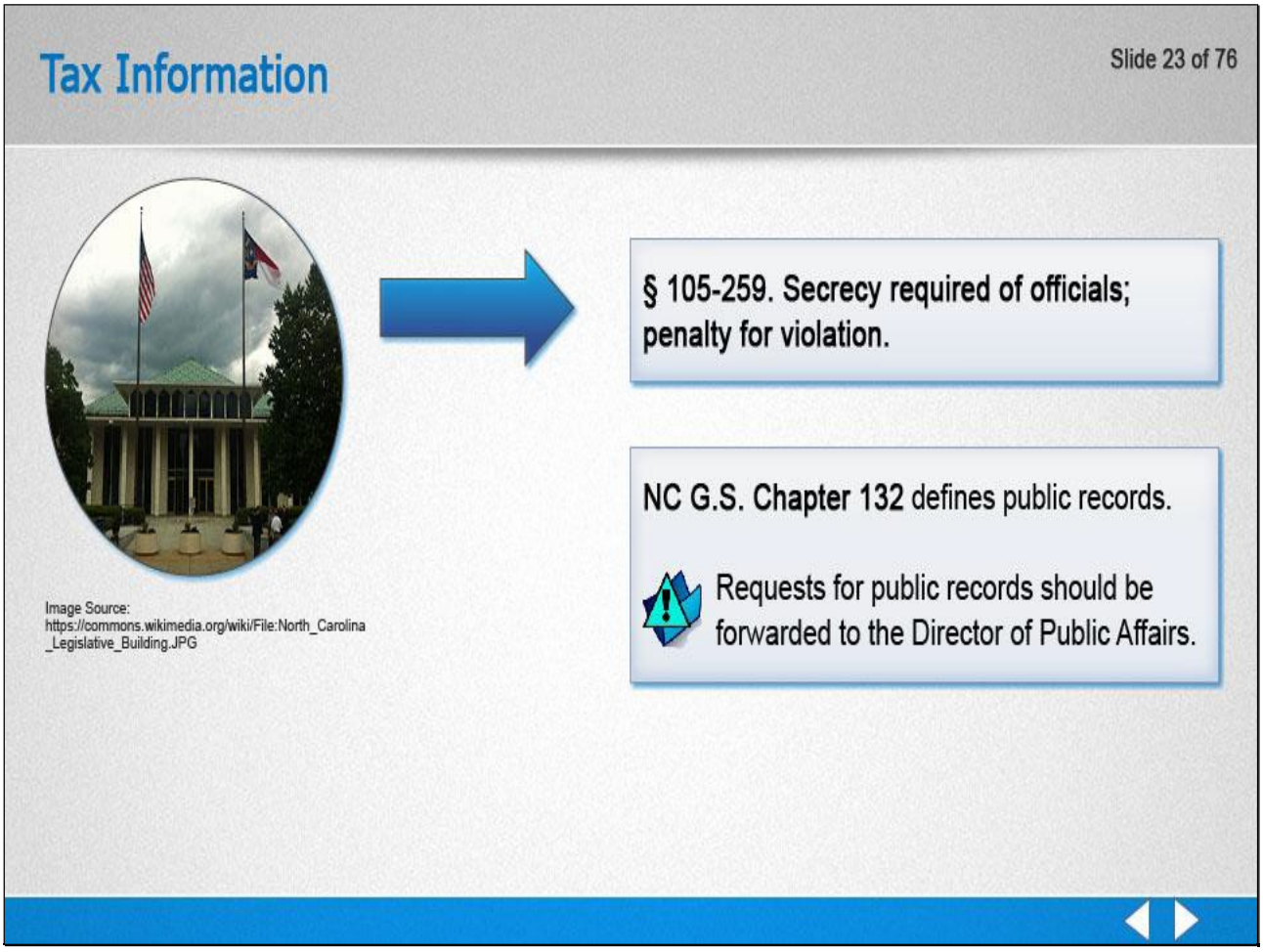
To begin, let's define what public records are.

Public records may include documents, paper, email, texts, or other means used to transact state business by any agency of North Carolina government, and are the property of the people.

Although these records are considered public property, there are limitations.

Public records do not include confidential or protected communications as defined in NC G.S. 105-259.

Tax Information



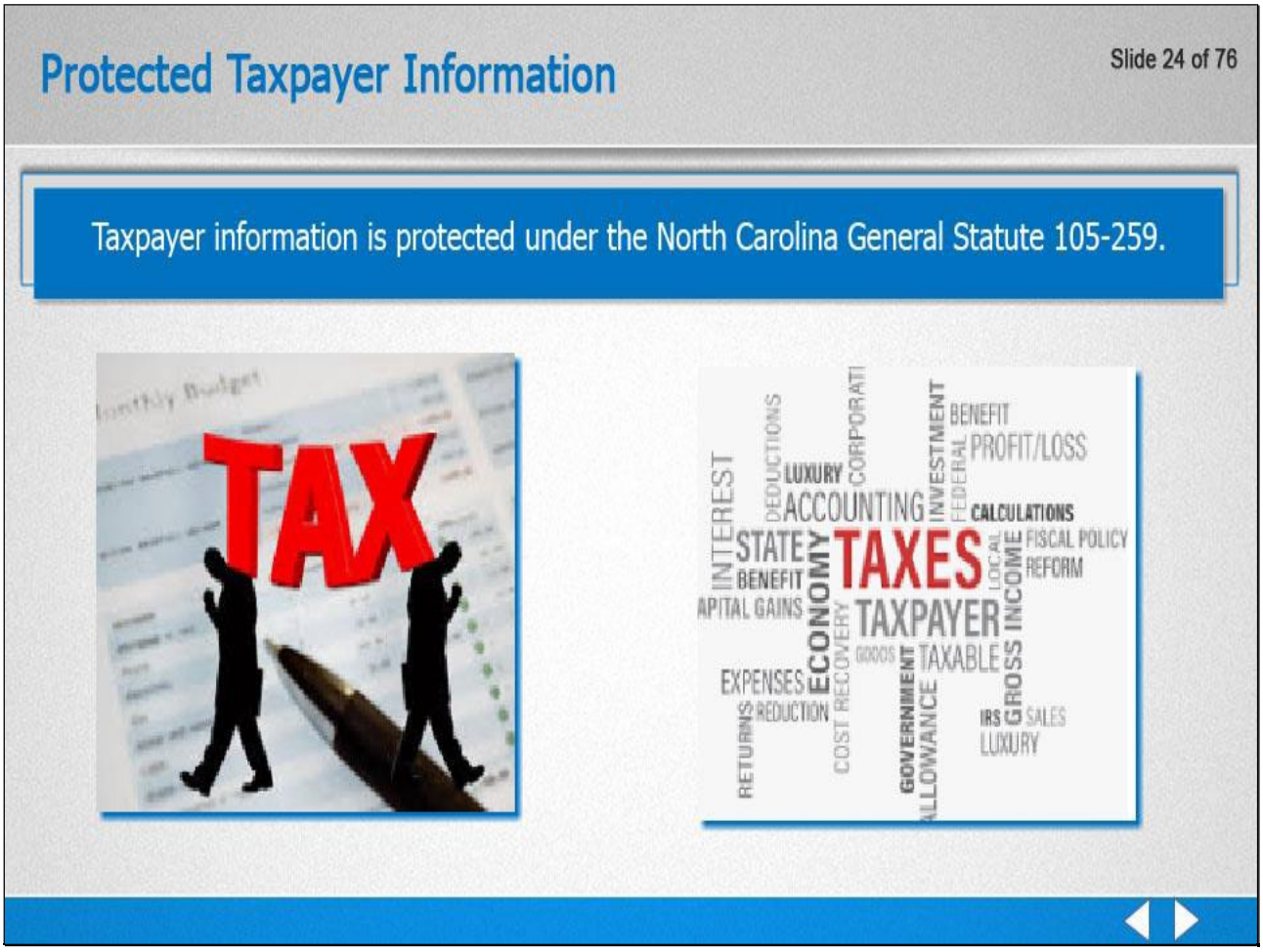
Notes

The North Carolina General Statute 105-259 also states that we may not disclose tax information to any other person unless the disclosure is specifically permitted by the statute.

NC G.S. Chapter 132 defines public records.

Therefore, if you receive a request for public records, please forward it to our Director of Public Affairs.

Protected Taxpayer Information



Notes

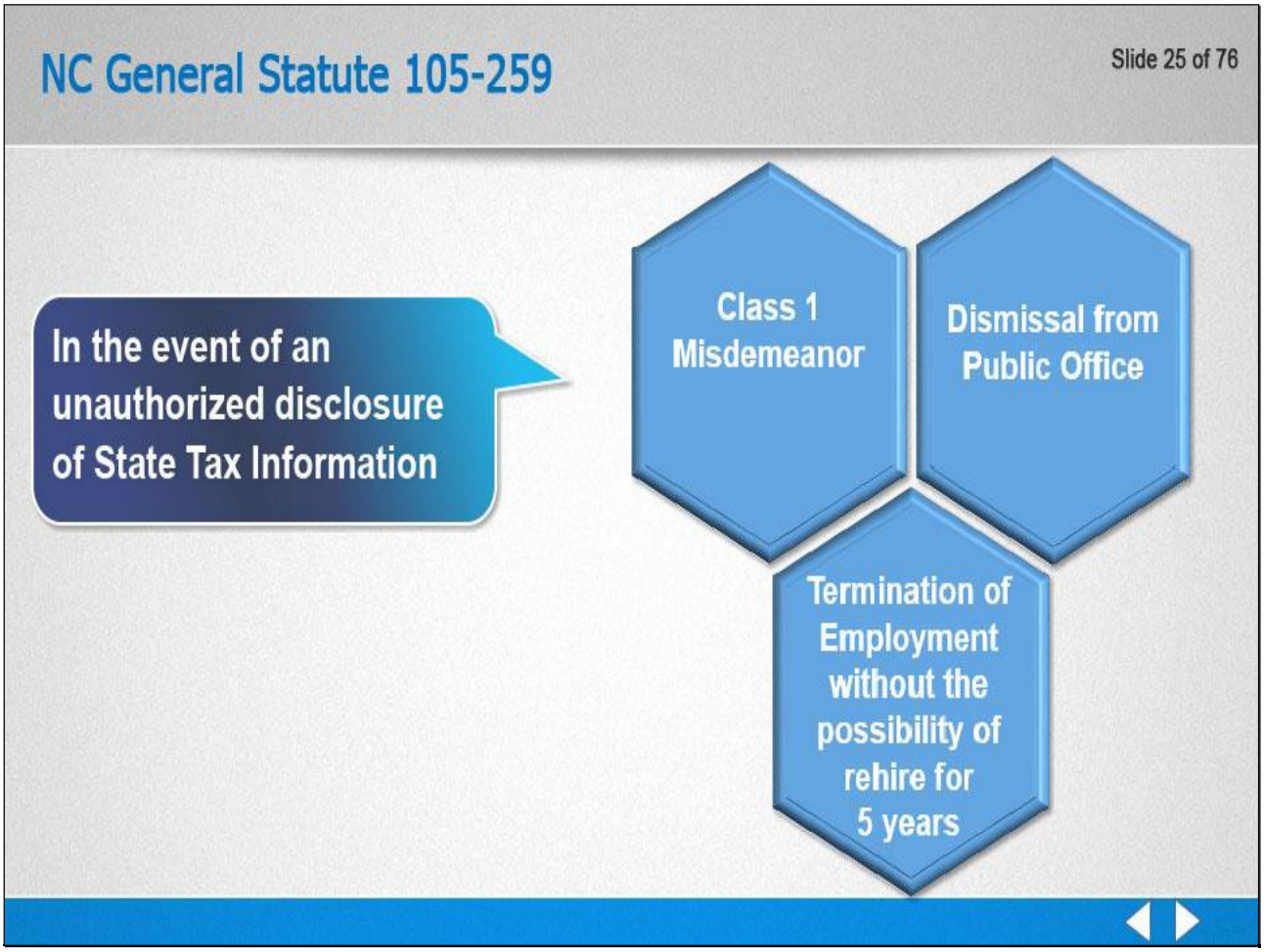
Taxpayer information is protected under the North Carolina General Statute 105-259.

Protected Tax Information includes the following:

- Information on a tax return, report, or an application for a license for which a tax is imposed
- Information from an audit of a taxpayer, or correspondence with a taxpayer, or information about whether a taxpayer has filed a tax return or report.

The North Carolina General Statute applies to current and former staff and officers, as well as to contractors.

NC General Statute 105-259

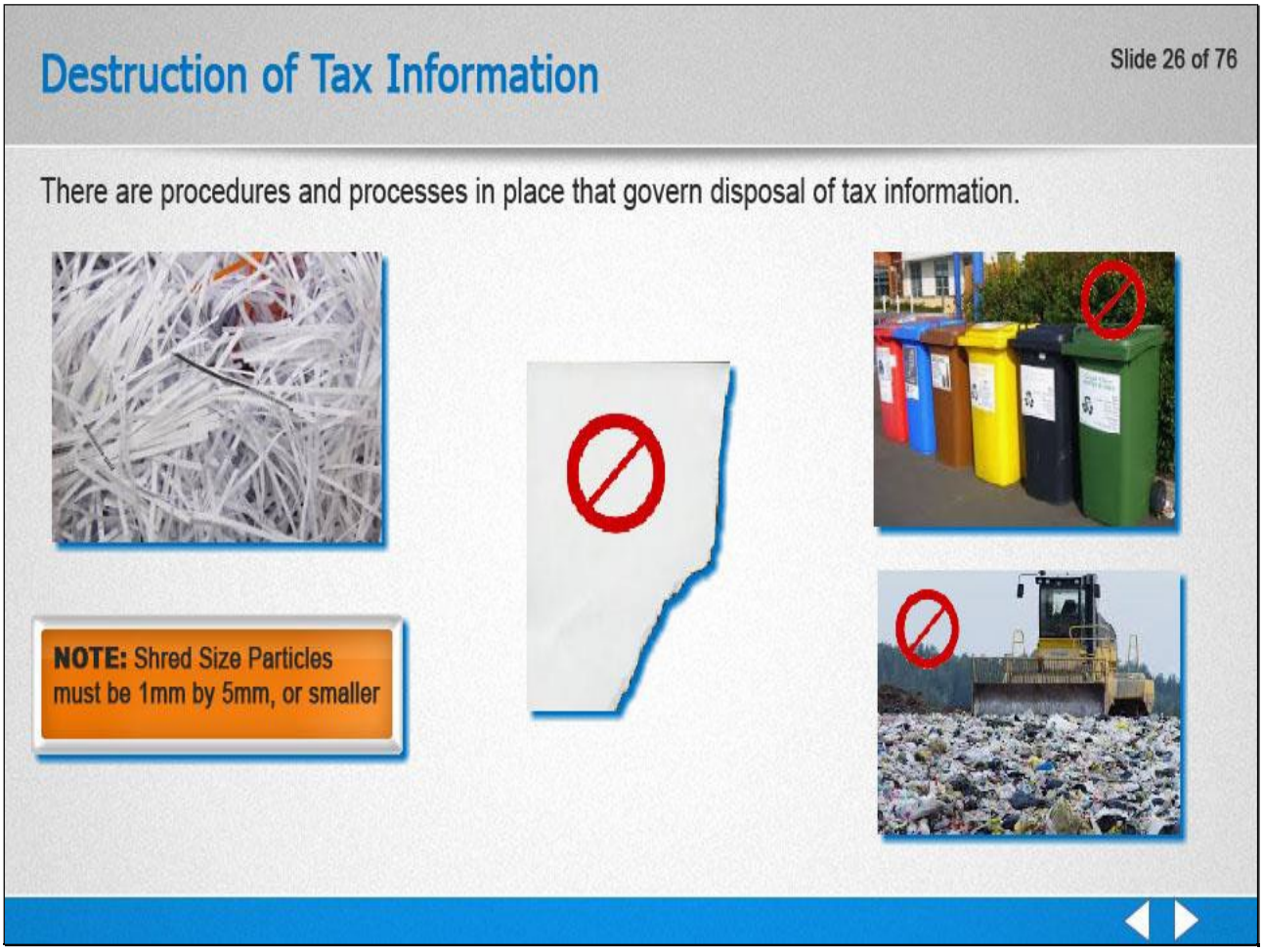


Notes

In the event of an unauthorized disclosure of State Tax Information in regards to the North Carolina General Statute 105-259, the following penalties may apply under North Carolina State Laws:

- Class 1 Misdemeanor
- Dismissal from Public Office, and
- Termination of Employment without the possibility of rehire for five years.

Destruction of Tax Information



Notes

Should the agency no longer need certain tax information, there are procedures and processes in place that govern the disposal.

Paper must be shredded using a cross-cut shredder. **NOTE:** Shred size particles must be 1mm by 5mm or smaller.

If shredding deviates from the above specifications, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.

Please Note: Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

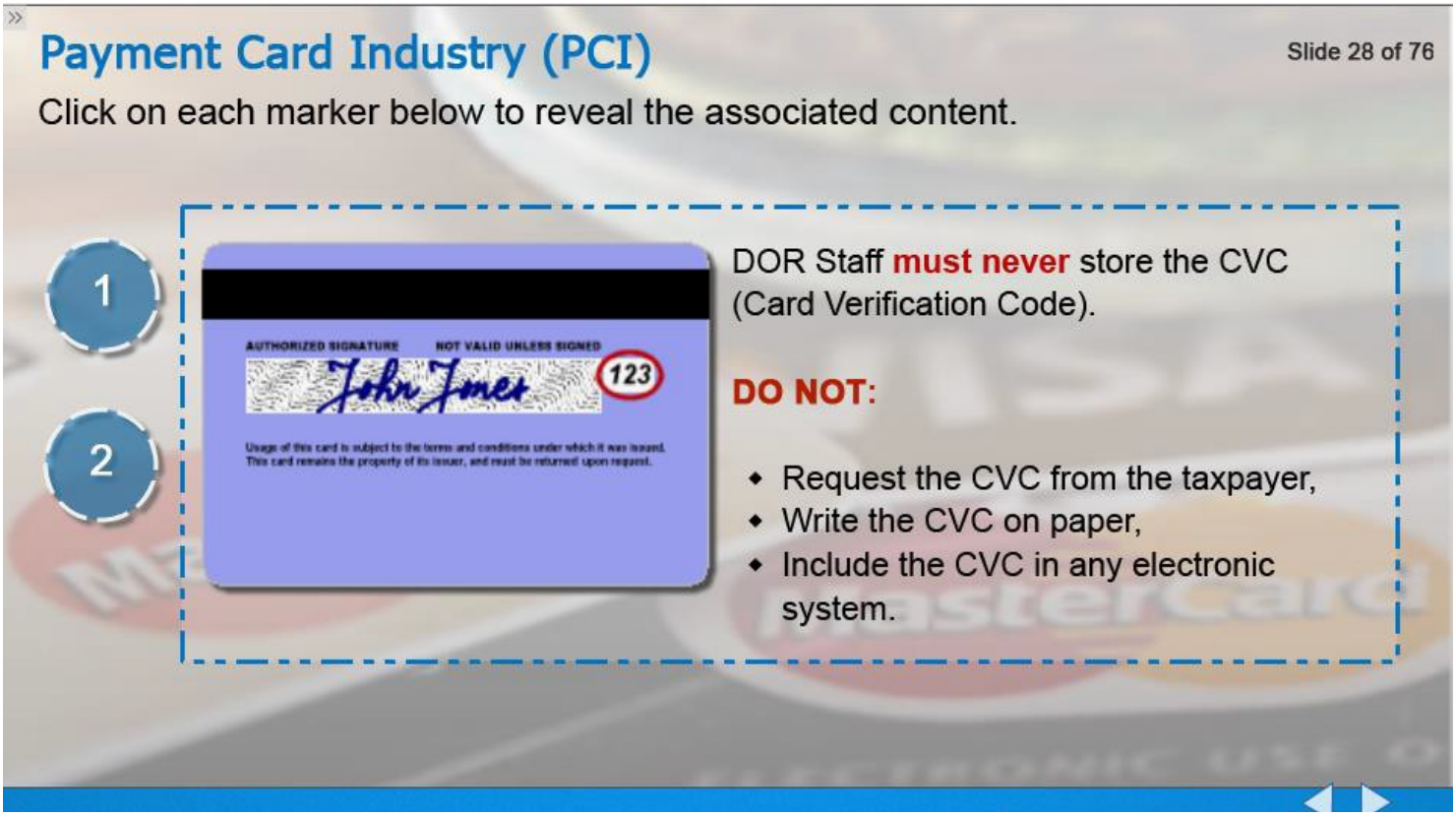
When in doubt about how to dispose of tax information, please contact the Chief Information Security Officer.

Payment Card Industry

Notes

Next, we will discuss some requirements of the Payment Card Industry that Revenue must adhere to.

Payment Card Industry (PCI)



Notes

In the event your job role requires a business need for you to collect credit card data from a taxpayer, certain precautions must be used in regard to handling and protecting this data.

You should never request the card verification code from the taxpayer, you must never store the card verification code, which is sometimes called the PIN verification code.

This is the 3 or 4 digit code found on the back of the credit cards or on the front of cards like American Express.

What does this mean?

It means that you should never write the card verification code on paper, even if you intend to destroy later.

You should never include the card verification code in any electronic system.

Payment Card Industry (PCI), cont.

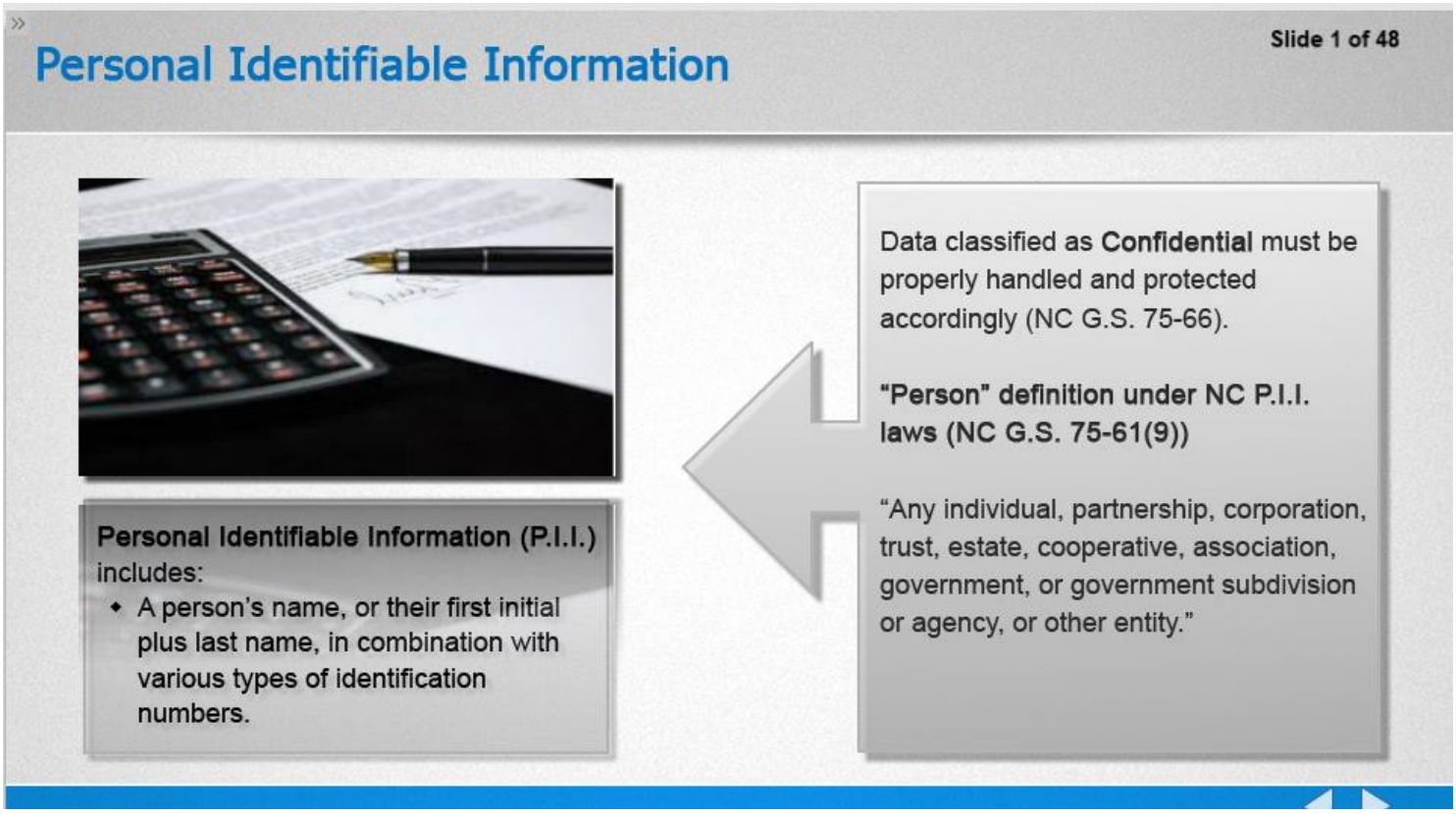
Notes

The Payment Card Industry allows us to store the 16 digit Primary Account Number, which is located on the front (or back) of the card, but it must be stored in an encrypted format.

Revenue stores this number encrypted, and this is handled by our IT Department.

If you need to dispose of the card information in printed format, remember that the cardholder data must be disposed of in a way so that it cannot be reconstructed.

Personal Identifiable Information



Notes

Personal Identifiable Information is information that includes: a person's first name or their first initial plus their last name in combination with various types of identification numbers.

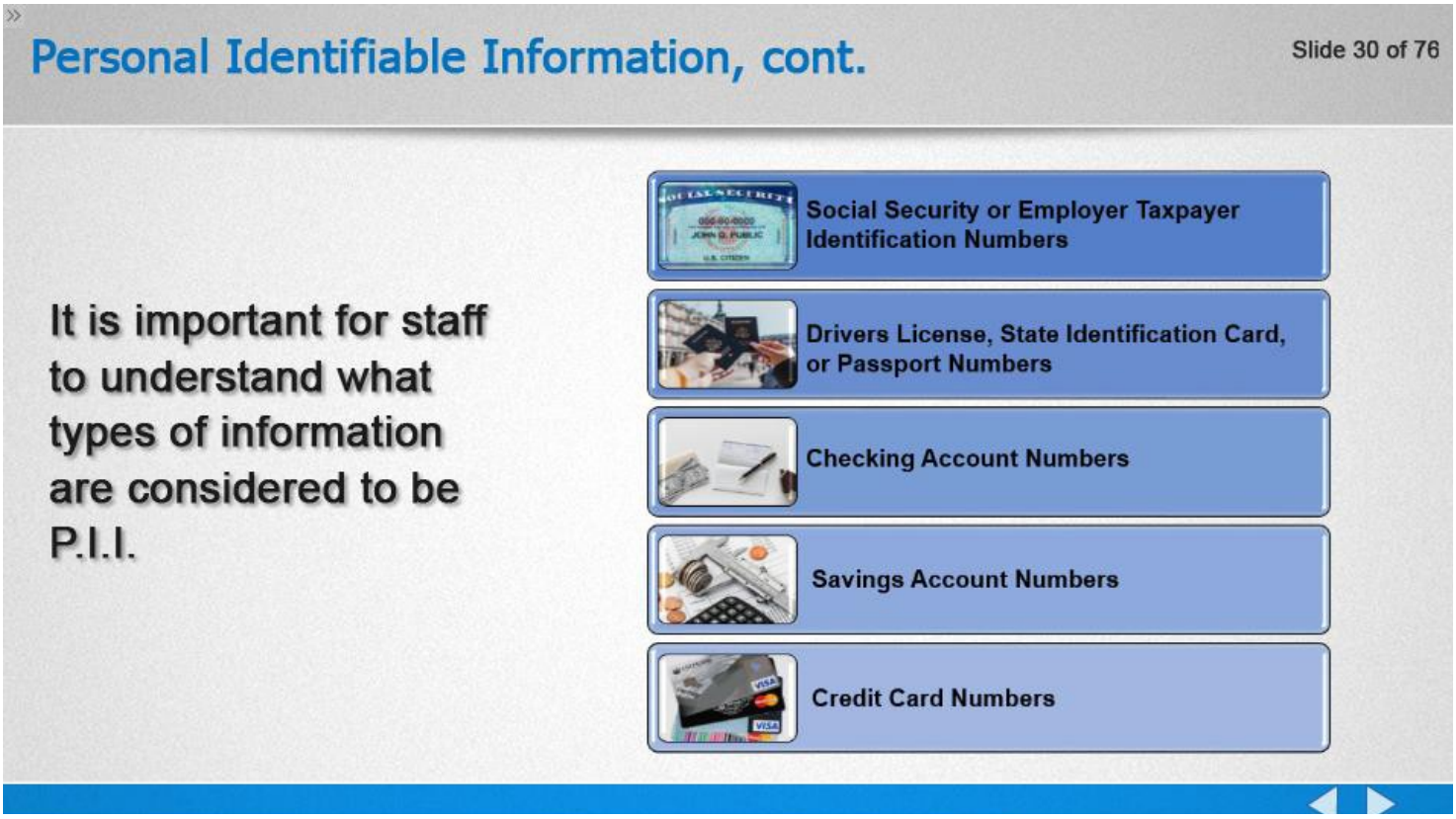
Under the North Carolina P.I.I. laws, business' information is also protected.

Because this type of data is classified as "Confidential," it must be properly handled and protected accordingly.

P.I.I. Laws define the word **person** as referring to an individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

An example of P.I.I. could include an individual's first and last name along with their social security number, or a business name and a tax identification number.

Personal Identifiable Information, (cont.)



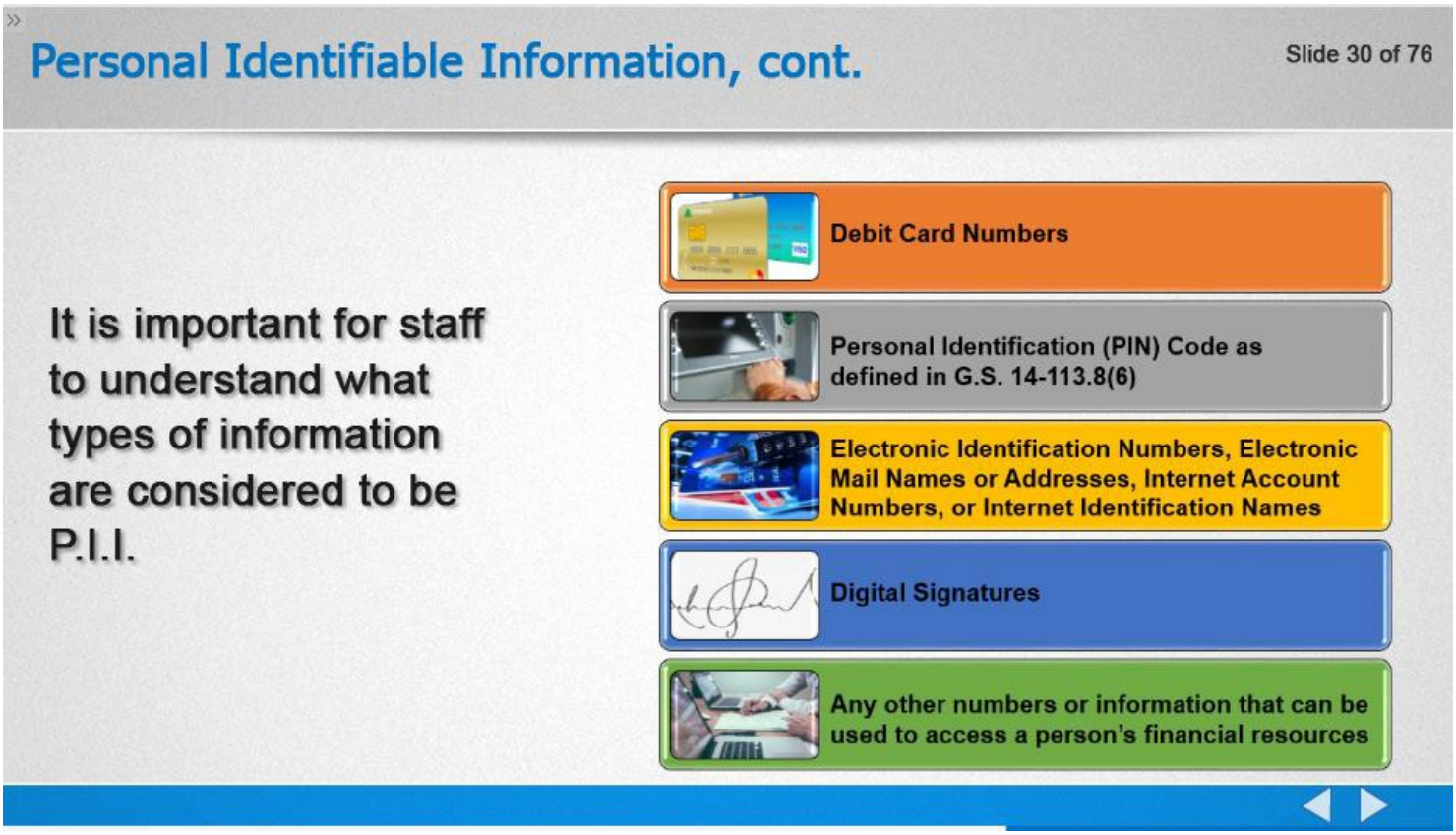
Notes

It is important that Staff understand what types of information are considered to be P.I.I.

Here is a listing of what Personal Identifiable Information may include under the North Carolina General Statute 14-113.20:

- Social security or employer taxpayer identification numbers
- Driver’s license, state identification card, or passport numbers
- Checking Account Numbers
- Savings Account Numbers
- Credit Card Numbers

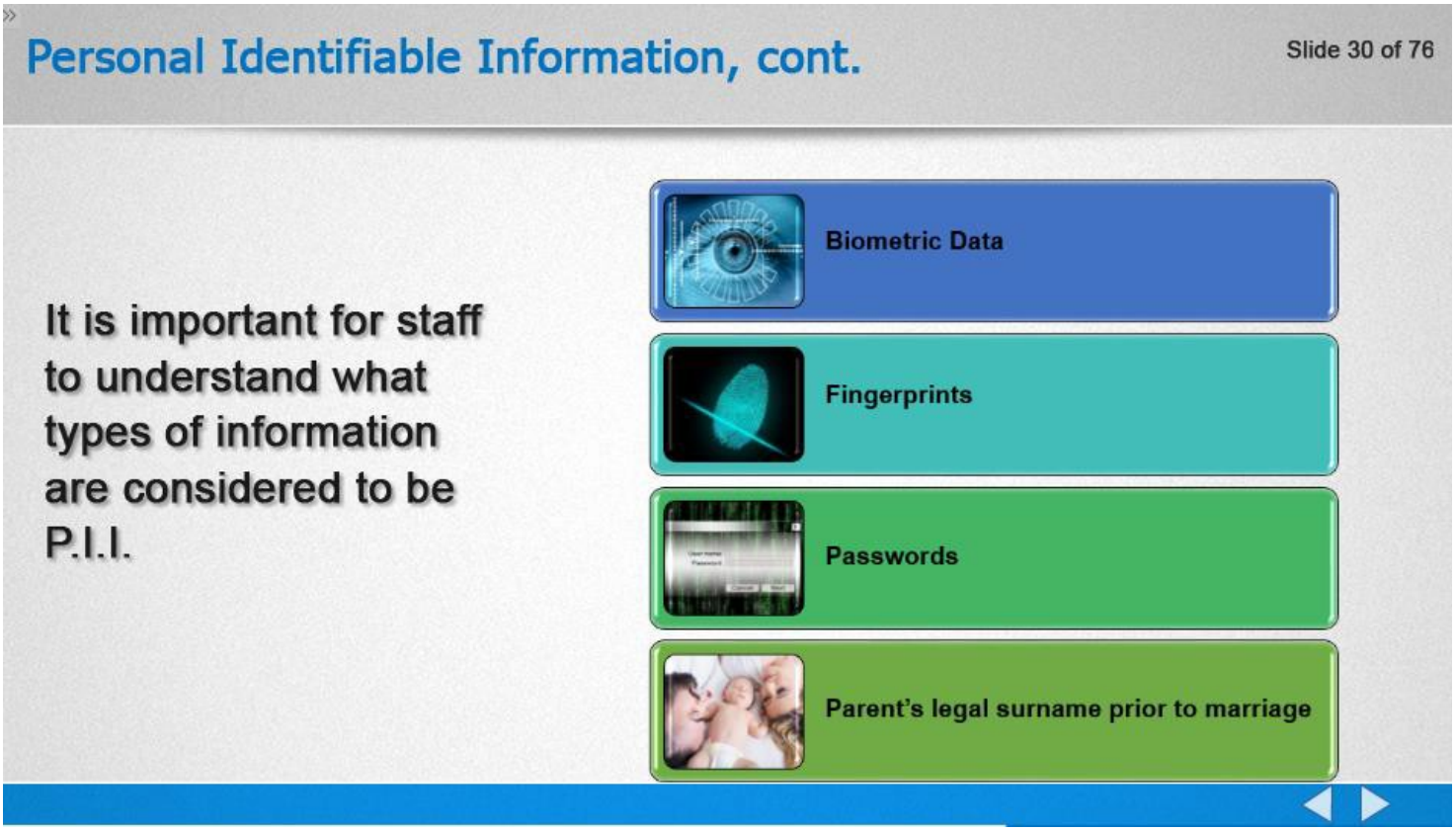
Personal Identifiable Information (cont.)



Notes, cont.

- Debit Card Numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- Electronic Identification Numbers, Electronic Mail Names or Addresses, Internet account numbers, or internet identification names
- Digital Signatures
- Any other numbers or information that can be used to access a person's financial resources.

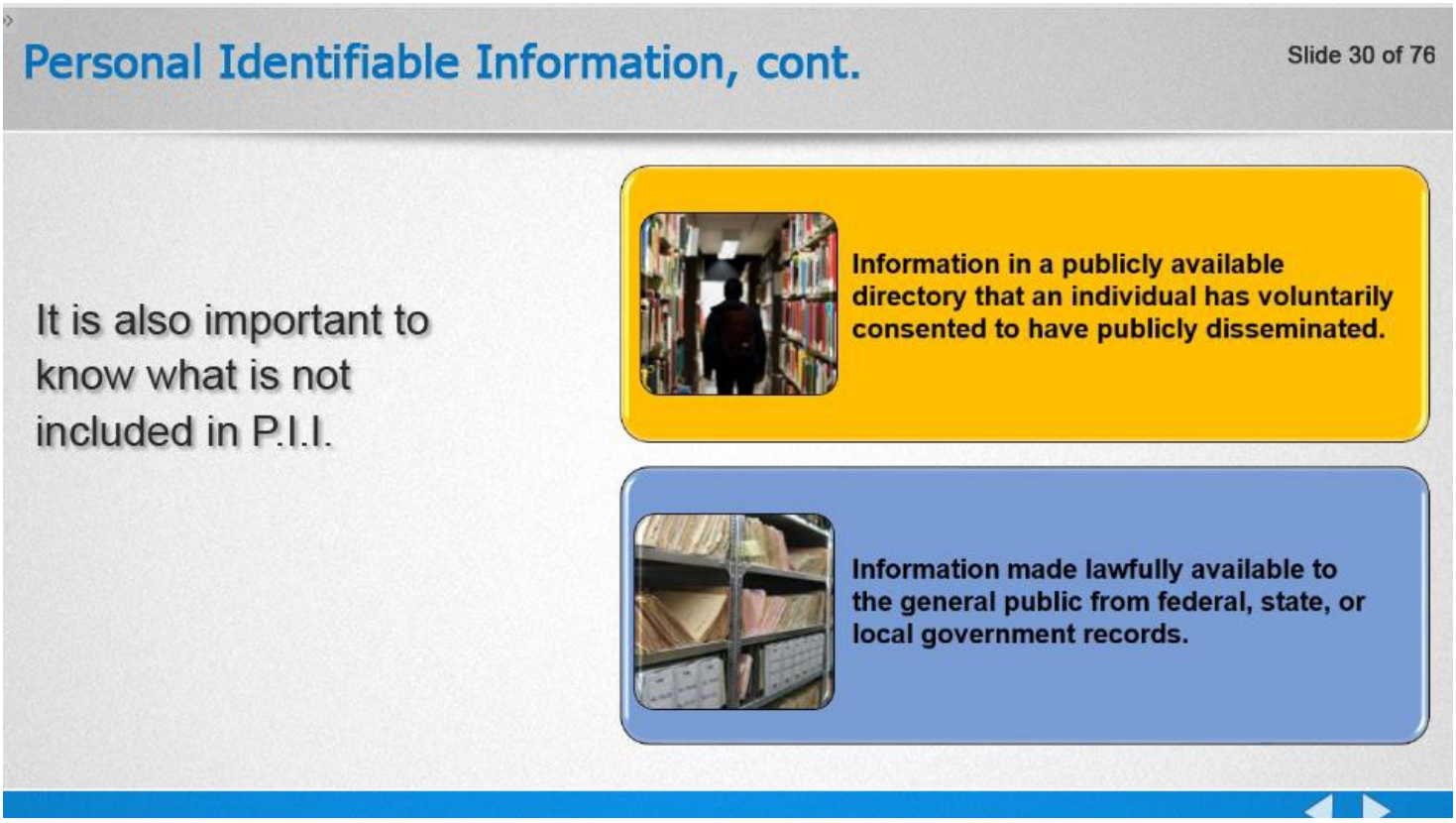
Personal Identifiable Information (cont.)



Notes, cont.

- Biometric data,
- Fingerprints,
- Passwords, and
- Parent's legal surname prior to marriage.

Personal Identifiable Information (cont.)



Notes, cont.

- Information in a publicly available directory that an individual has voluntarily consented to have publicly disseminated.
- Information made lawfully available to the general public from federal, state, or local government records.

All Possible

Notes

The last data classification we will look at is “All Possible.” Occasionally you may run across data that is classified as “All Possible.” This is the highest classification that we have here at DOR.

What this means is that all of the regulations and requirements that the Agency is expected to follow should be applied to this data.

Staff Security Responsibilities

Notes

This section of the training covers insider threats.

On the next slide, review the video transcript from David Roseberry discussing some primary ways internal threats may occur within the agency.

Internal Threats

Video Transcript

So, there's also internal threats, that's primarily from us. Two primary ways mostly is going to be accidental, leaving your computer unlocked, and walking away, you have a laptop, you go to a conference, and turn away from what you're looking at on the screen to talk somebody beside you, and all of a sudden you may have exposed some information, you didn't mean to, but you exposed the information and somebody may be waiting for you to do just that right.

So, we want to be careful about what we're doing and just be aware of our environment as well. But it could also be people who have fallen on hard times internally and may decide to pick up a check or money order they have access to, or they just go to a party and go well "Hey, I know how your taxes are performed." These are the audit methods that we use. I found some interesting information about my neighbor, I know how much money they make, if you want to know something, let me know, and I can help you out with that. So that's kind of what the internal threats look like here.

Staff Security Responsibilities

Video Transcript

The security of data, as well as the safety of agency staff members is the responsibility of everyone.

Here are a few security responsibility reminders for all staff:

- Staff members should always be aware and observe their surroundings, and they should report any security violations to the Service Desk.
- There is no expectation of privacy when using Revenue owned resources.
- Protect, and do not share your logon credentials.
- Do not change any security settings of resources.
- Staff members should not put any offensive, libelous, harassing, or discriminatory statements into electronic communications such as text messages or emails.
- Do not attempt to access data, resources, or media that is not appropriate for your duties or which you are not authorized.
- Immediately report to the Service Desk any discovered access to resources or data that is not appropriate for yourself or staff members.
- Report any suspicious behavior that might indicate an insider threat to the Service Desk.

Let’s discuss an insider threat next.

Staff Security Responsibilities, cont.

Video Transcript, cont.

Recognizing potential indicators of insider threats

An Insider Threat is a malicious threat to an organization that comes from people within the organization.

It is important that all staff know how to recognize potential indicators of an insider threat. You must report all suspected insider threats to the Service Desk.

Some behaviors that you may observe in the individual include:

- Violating agency policy
- Showing disregard for rules
- Working odd hours without authorization
- Unnecessary copying of material, especially if it is proprietary or classified
- Interest in matters outside the scope of their duties

Due to the serious nature of an Insider Threat, the DOR asks:

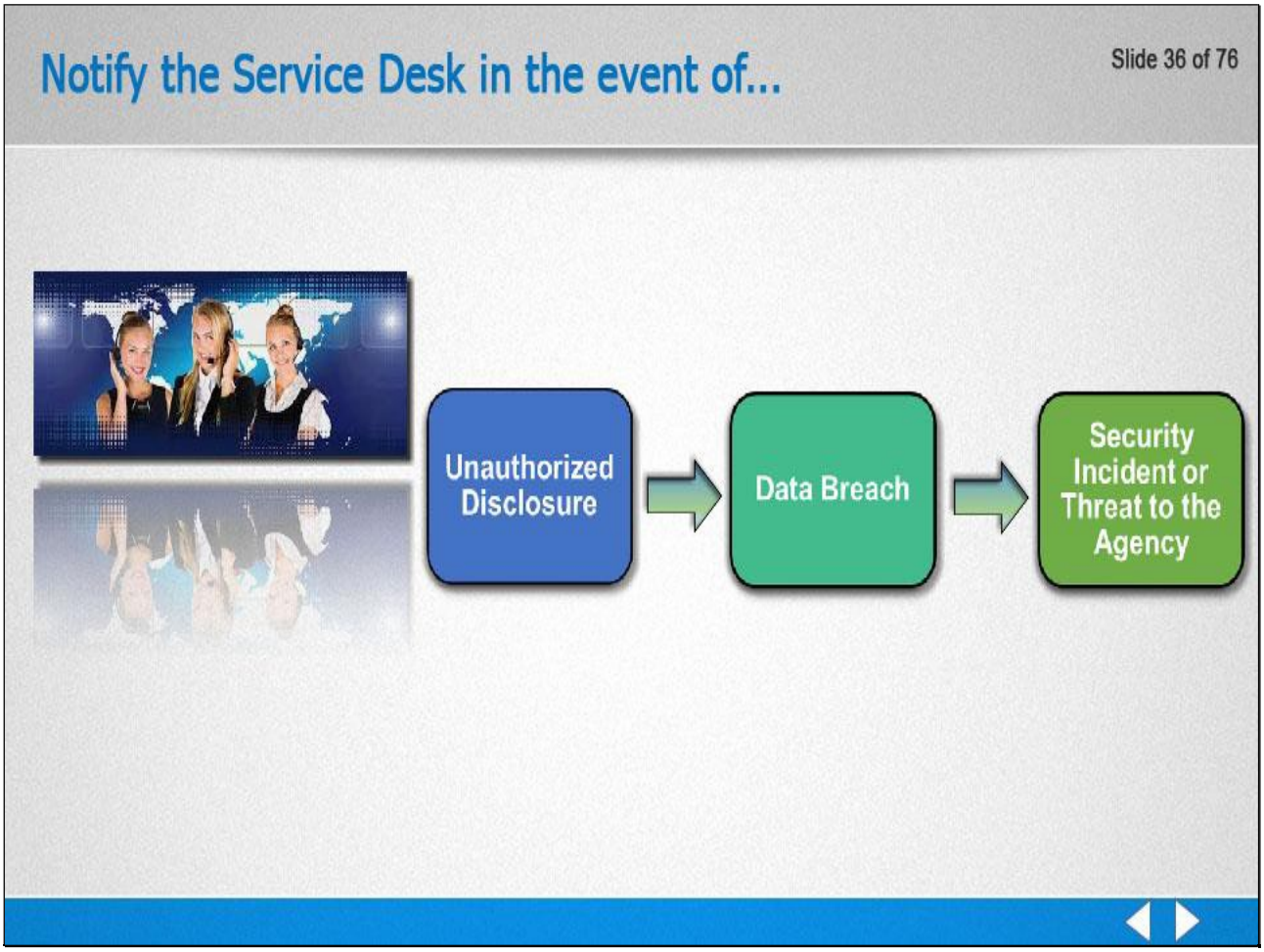
- All personnel to be mindful of the potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform malicious actions, which could include, but is not limited to, the unauthorized access or re-disclosure of FTI.
- All suspected Insider Threats must be reported to the NCDOR Service Desk.

Here are some different ways you can help to prevent threats to the Agency:

If you are a manager and need to request access for your team members, remember, you should only request the least amount of privileges needed for your staff to perform their job duties. Always verify the identity of any third-party persons (for example, people claiming to be repair or maintenance personnel), prior to granting them access to any area of the facility or to modify or troubleshoot any resource.

In the event of a staff member termination, or other separation of service, report it immediately to the security guards and the service desk.

Notify Service Desk



Notes

Information Security Incident Management Policy and Plan:

Notify the Service Desk immediately in the event of:

- **Unauthorized Disclosure**: an event involving the exposure of information to entities not authorized to access the information.
- **Data Breach**: An incident in which sensitive, protected or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.
- **The discovery of any suspected Security Incident or threat to the Agency**.

Staff Security Responsibilities

Notes

Although agency staff members have access to the Internet, please remember the following safety precautions:

- Internet usage is monitored for all staff members.
- Do not download any software without prior approval from the Chief Information Security Officer.
- Any approved files downloaded from the Internet must be scanned for viruses.
- No Federal Taxpayer Information or Confidential information shall be transmitted over the Internet without prior approval of the Chief Information Security Officer.

This is to ensure the communication is approved and is sent using approved secure methods.

Staff Security Responsibilities, cont.

Notes, cont.

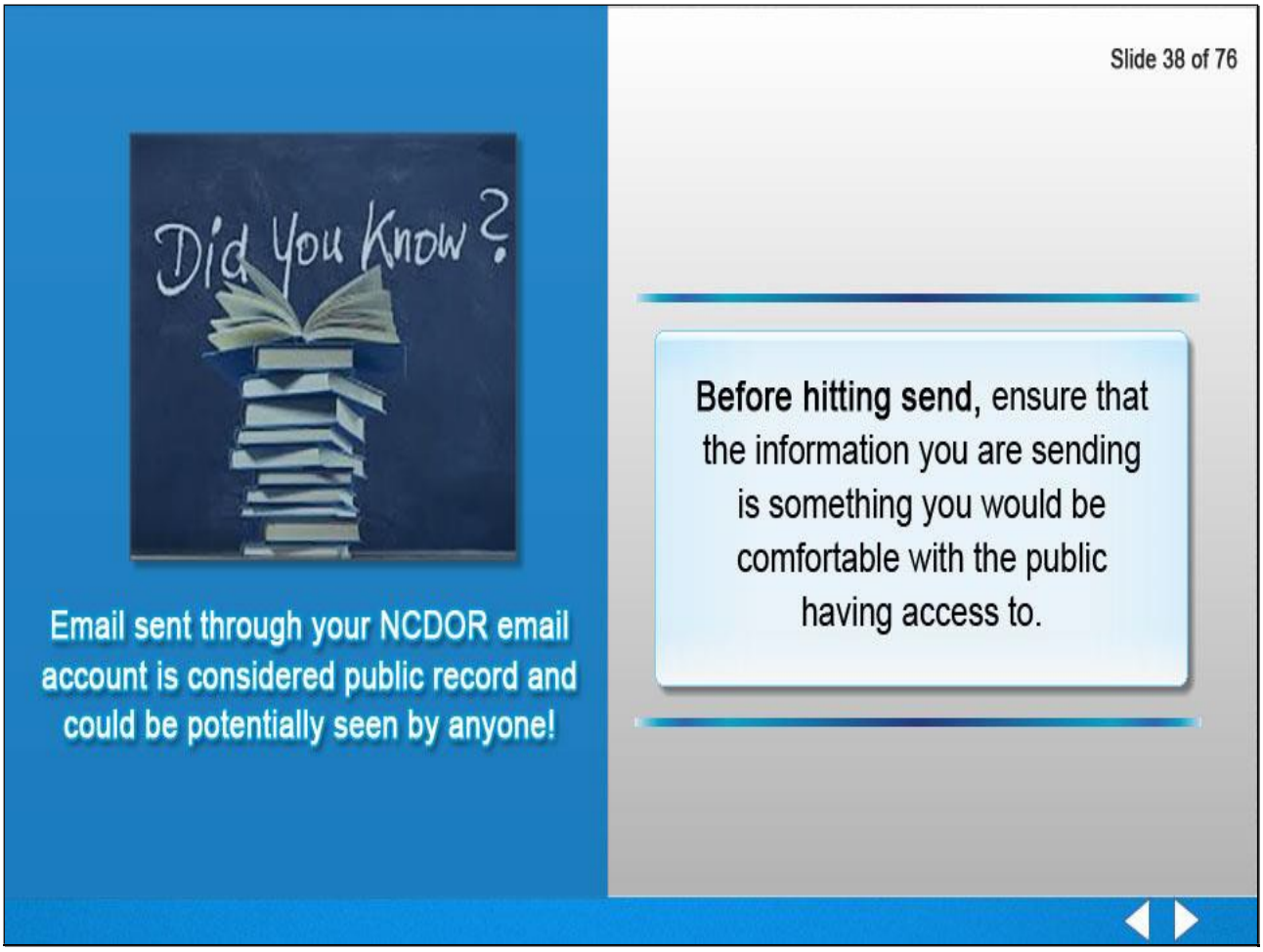
All Internet email accounts, such as Hotmail, Gmail, and Yahoo are prohibited at Revenue.

And when using a messaging system, please remember

Confidential information and FTI should only be disclosed to authorize participants with an established business need, and the information must be used for processing a valid business request.

All messages are subject to North Carolina Public Record laws.

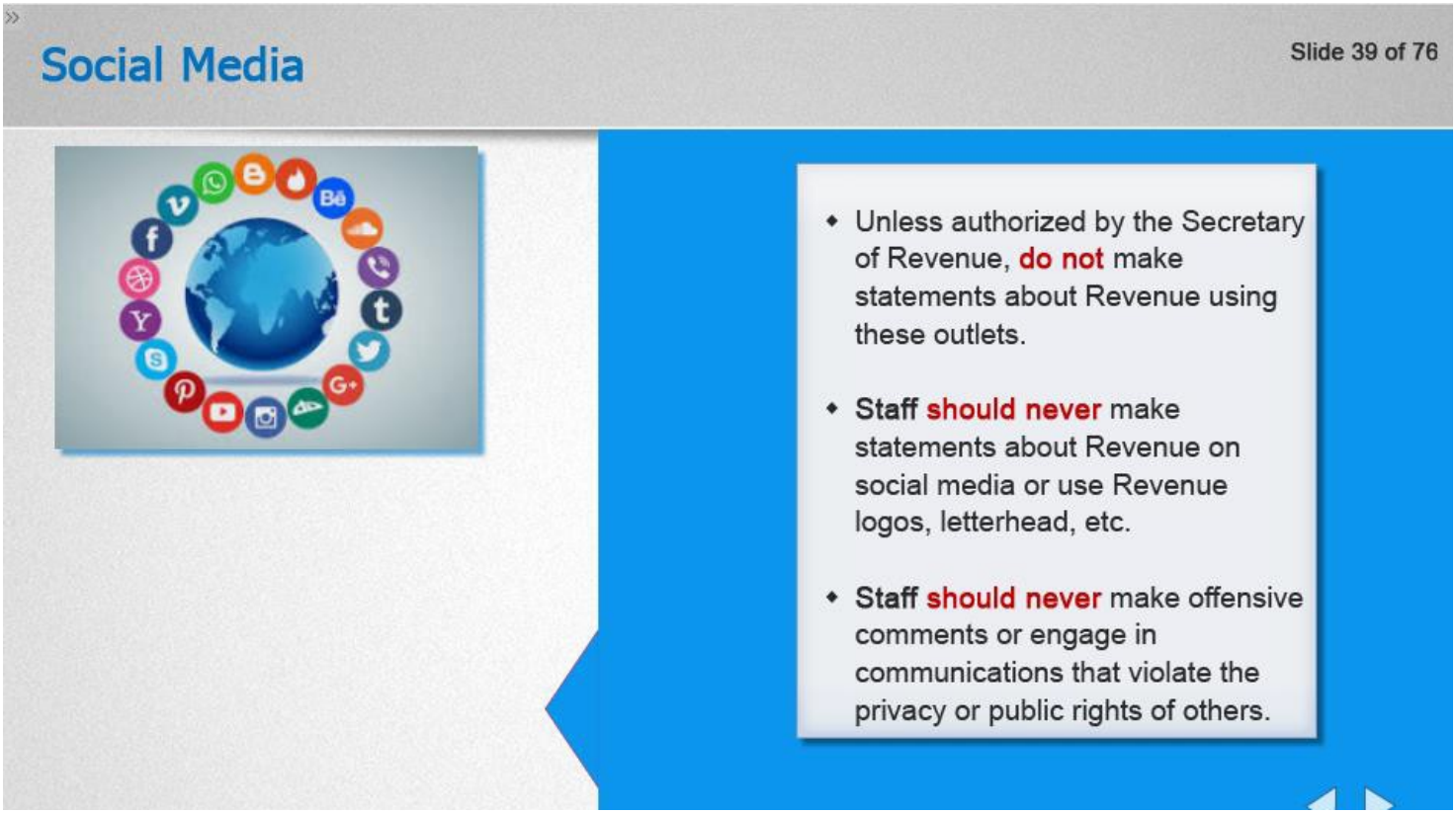
Did You Know



Notes

Did You Know - Emails are considered to be public record. Before hitting send, ensure that the information you are sending is something you would be comfortable with the public having access to.

Social Media

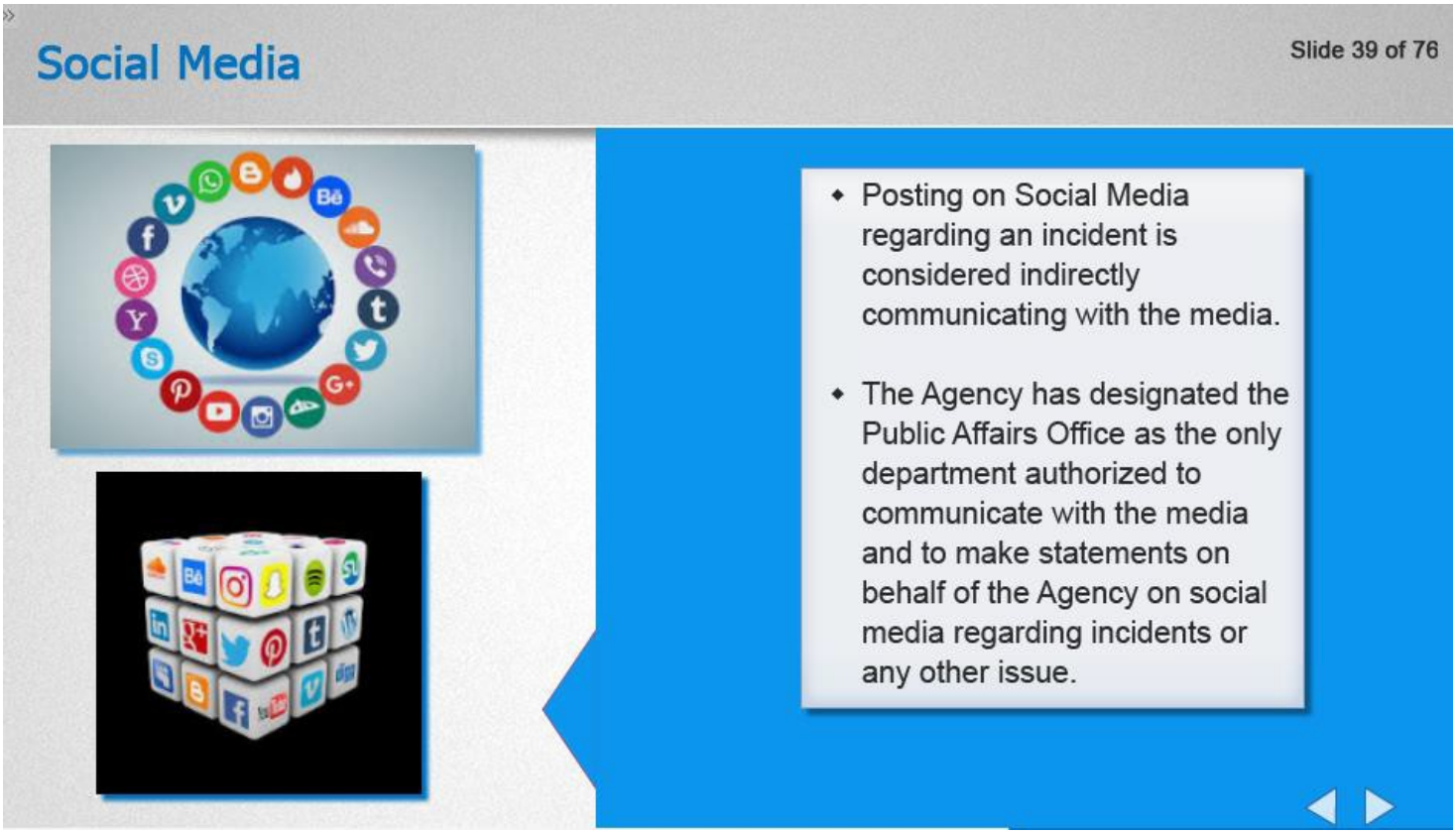


Notes

There are many social media outlets and all are easily accessible.

- However, unless you are authorized by the Secretary of Revenue, do not make statements about Revenue using these outlets.
- Also, do not use Revenue logos or letterheads without prior approval.
- Revenue staff should never make any offensive comments or engage in communications that violate the privacy or public rights of others.

Social Media, cont.

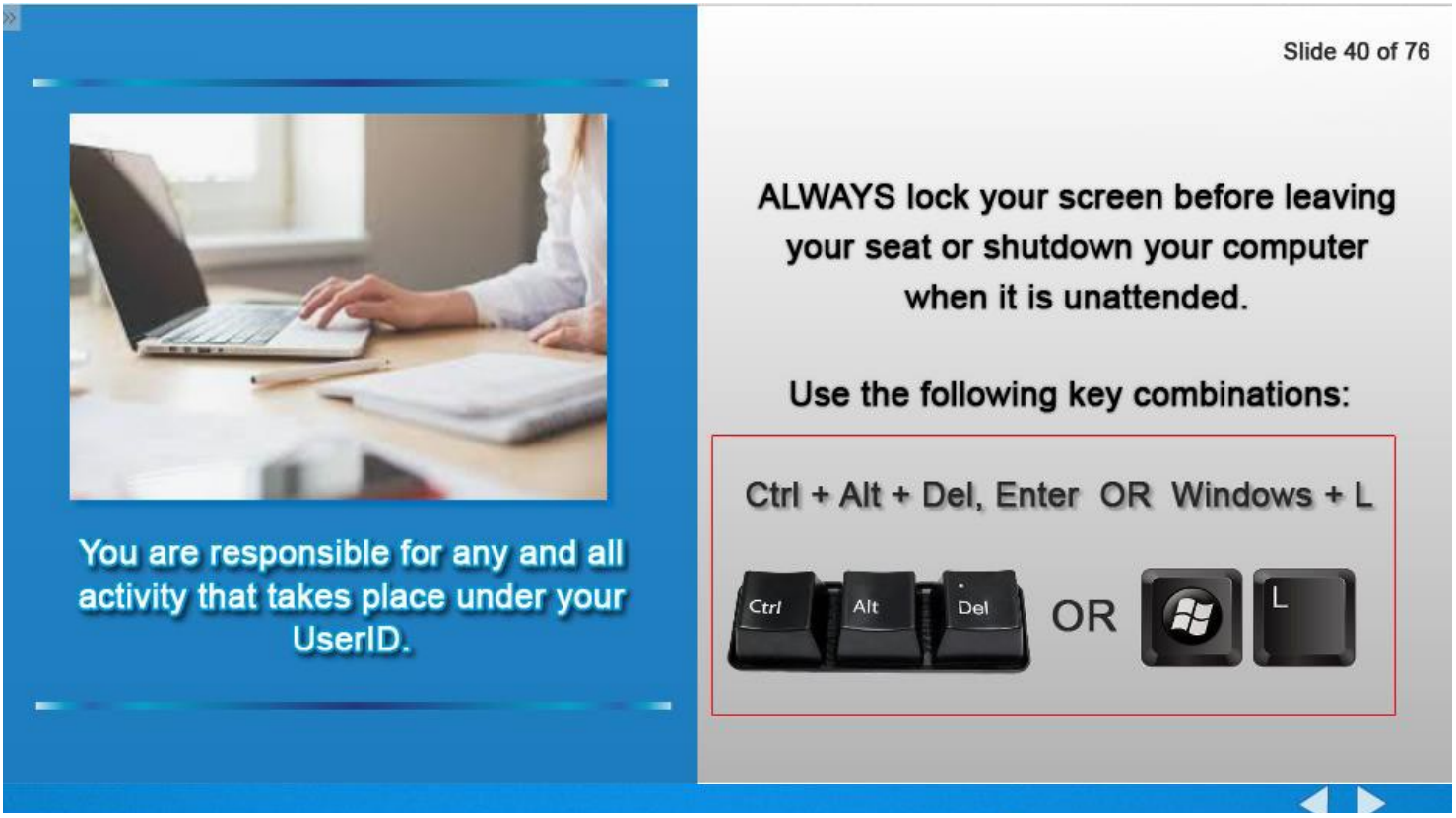


Notes, cont.

Posting to Social Media regarding an incident is considered indirectly communicating with the media.

The Agency has designated the Public Affairs Office as the only department authorized to communicate with the media and to make statements on behalf of the Agency on social media regarding incidents or any other issue.

Staff Security Responsibilities



Notes

Along with creating and using strong passwords, you can also protect the access of information by locking your computer.

Because you are responsible for any activity that takes place under your User ID, it is required that before you leave your seat, always lock or shut down your computer when unattended.

You can lock your screen by using the following key combinations:

- Control, Alt, Delete and then the Enter key, or
- Press the Windows key and the L key. (Refer to the example provided on the slide.)

By taking these appropriate measures, it will help to safeguard not only yourself, but also taxpayer information.

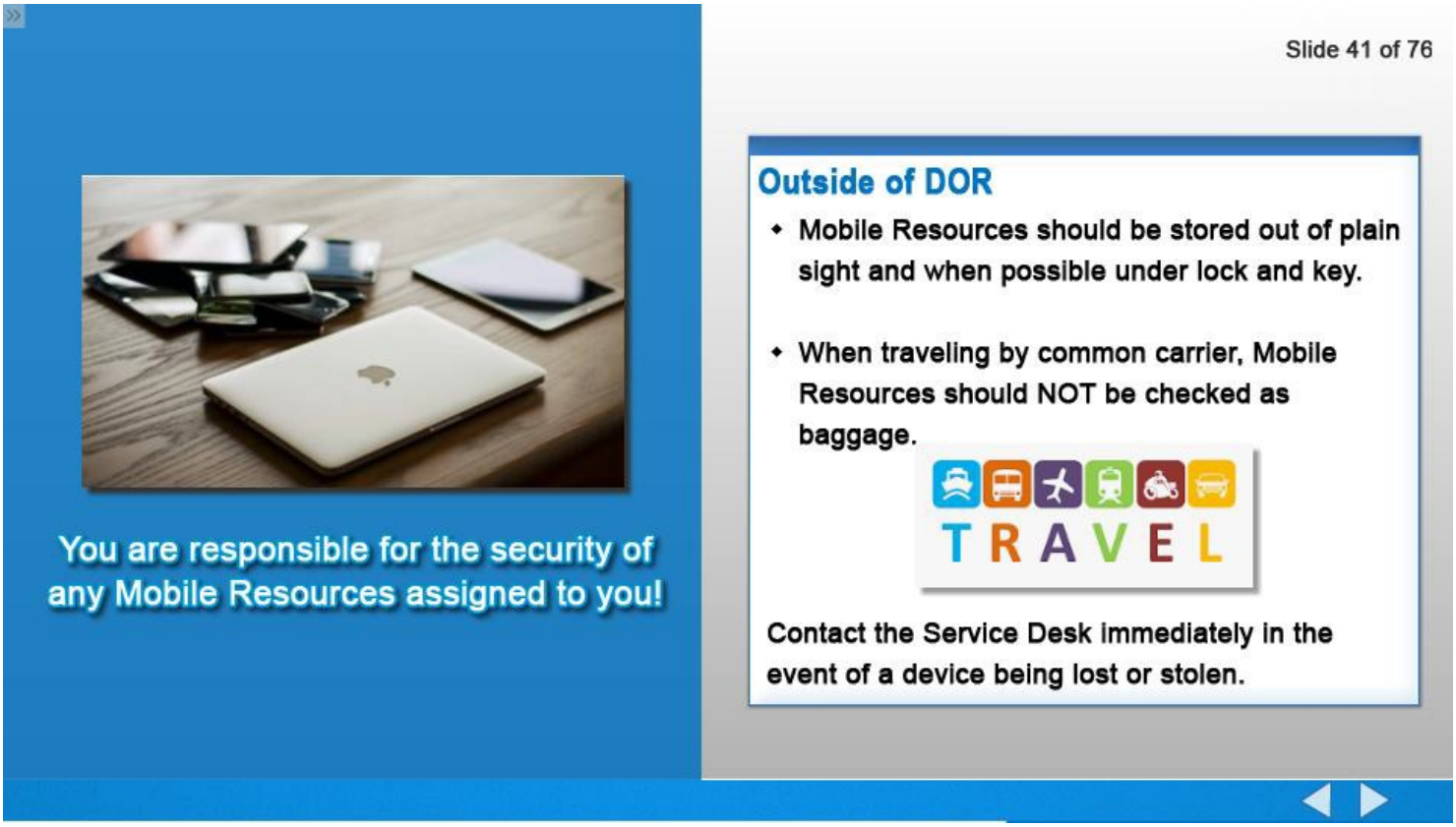
Staff Security Responsibilities

Notes

If any mobile resource has been assigned to you, for example, laptops, smart phones, or tablets, you are responsible for their security.

All mobile resources are considered secure while inside Revenue facilities, unless otherwise indicated.

Staff Security Responsibilities, cont.



Notes, cont.

While outside of Revenue facilities, mobile resources should be stored out of plain sight and when possible under lock and key.

When traveling by common carrier, for example, airplane, train, bus, or boat, mobile resources should not be checked as baggage.

Staff Security Responsibilities, cont.

Notes, cont.

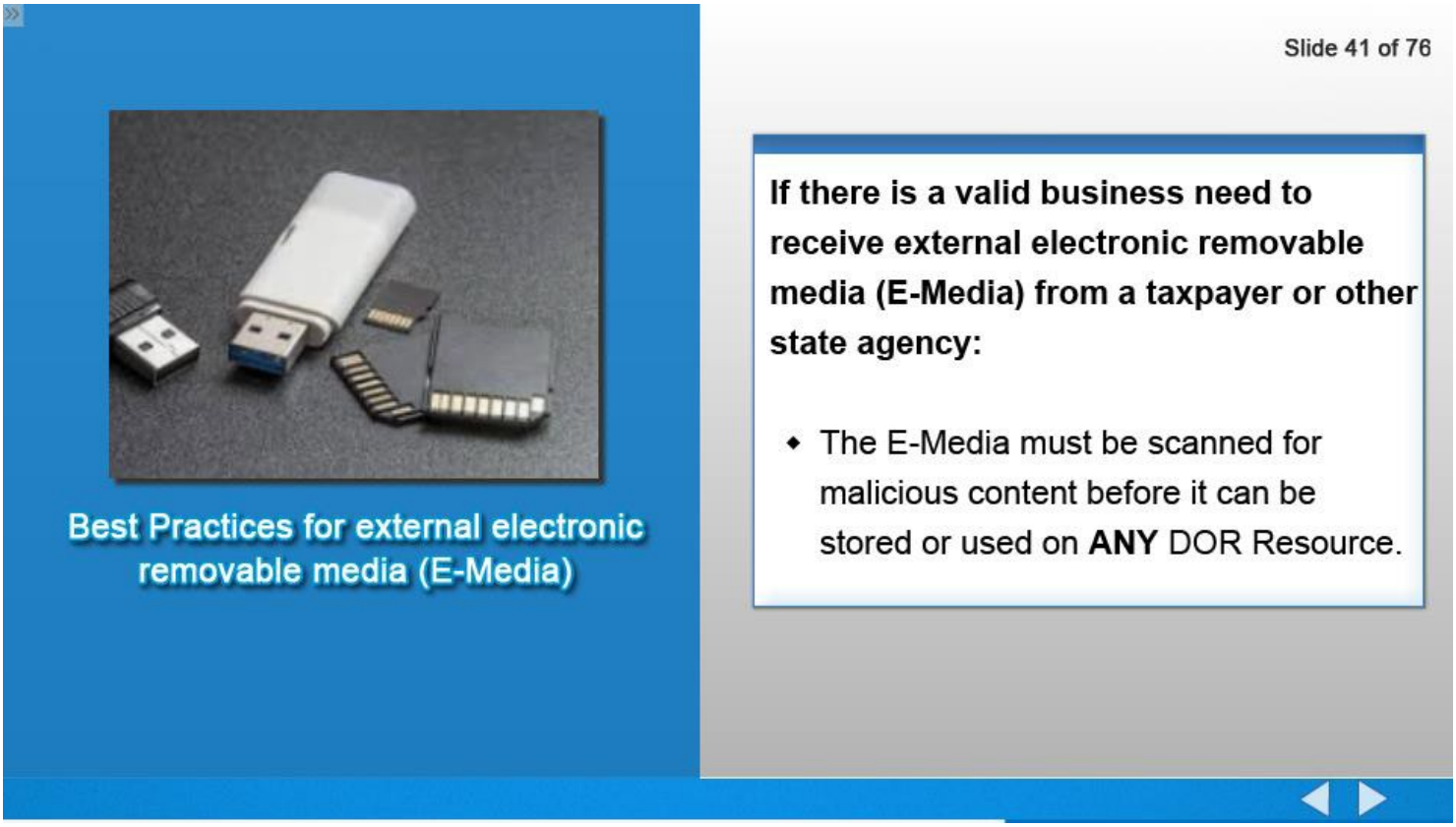
To prevent the possibility of system viruses, do not install or connect any non-Revenue issued hardware or media to any Revenue device or to the Revenue network.

When in doubt, here is an easy way to remember: if Revenue did not issue it to you, do not put it into a Revenue computer.

The only exception is if there is a valid business need, and proper precautions, such as virus scanning has been performed prior to connecting it to the Revenue network.

Examples of hardware and media may include: CDs, Modems, Flash Drives, MP3 Players, Personal Data Devices, iPods, and smart phones.

Staff Security Responsibilities, cont.

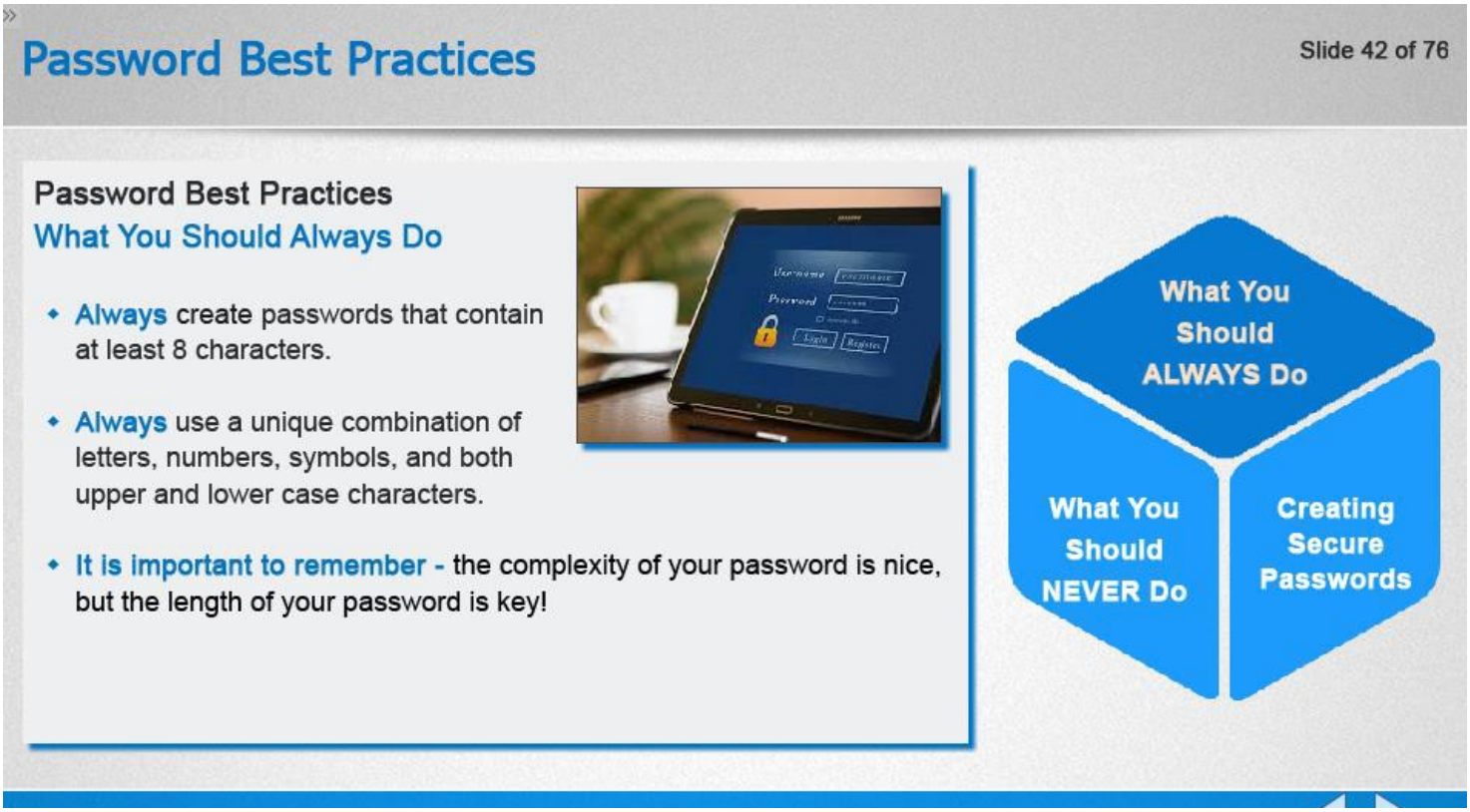


Notes, cont.

If there is a business need that requires you to receive external electronic media, such as a CD,

USB drive, or Flash drive from a taxpayer or other state agency, remember that all electronic media must be scanned for viruses before being stored or used on any Revenue system.

Password Best Practices



Notes

For the safety and security of the data housed at Revenue, our systems require passwords, and in some cases, multiple passwords to access information.

To improve the security of system passwords, they should be complex and contain at least 8 characters utilizing a combination of upper and lower case letters, numbers, and special characters.

Remember, the complexity of your password is nice, but the length of your password is key.

Password Best Practices, cont.

Notes

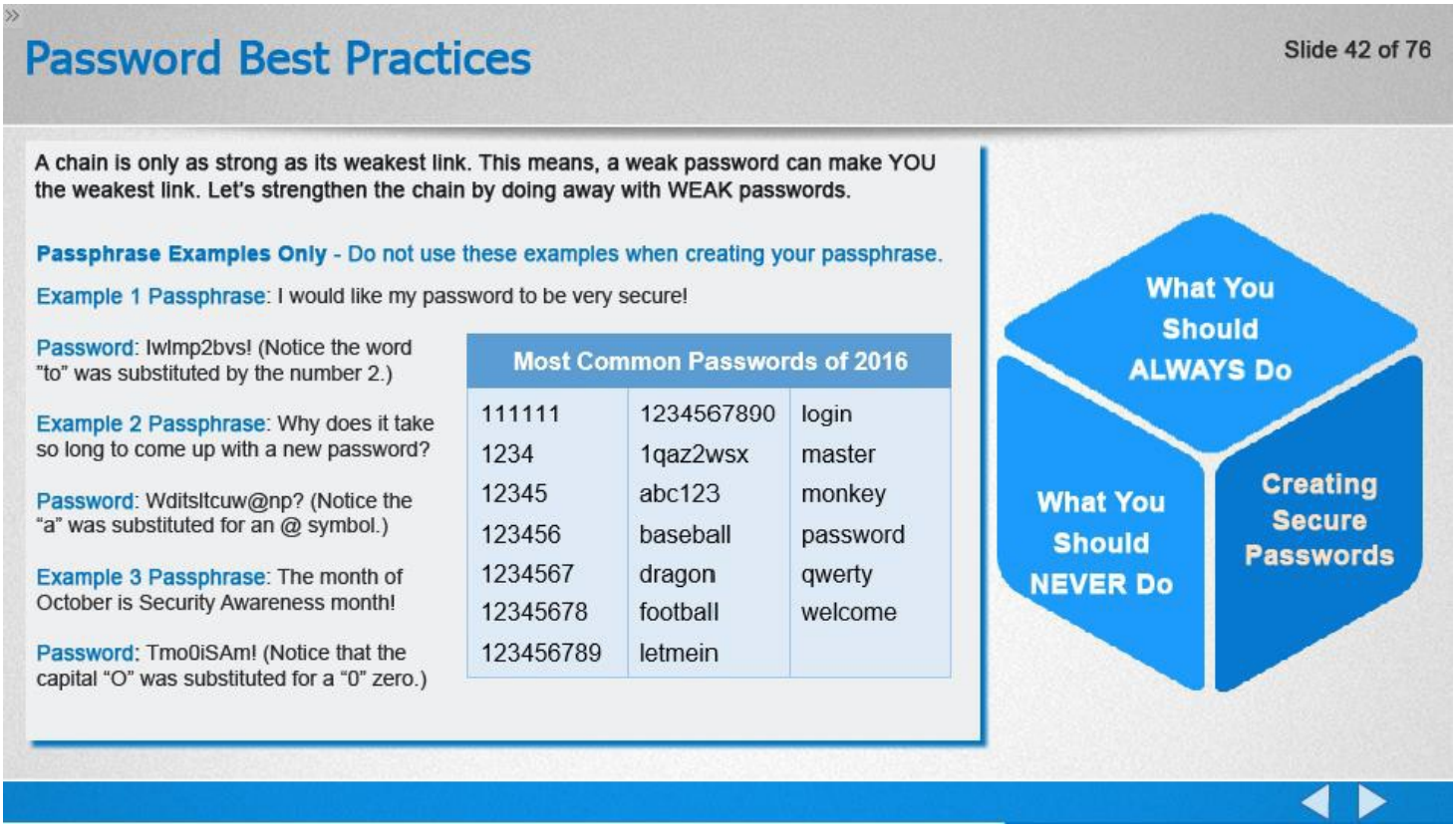
Now let's discuss some more password best practices, in regard to password safety.

Revenue staff should not share passwords with other staff members, store their passwords in any electronic communication, or embed their passwords in automated programs, utilities or applications.

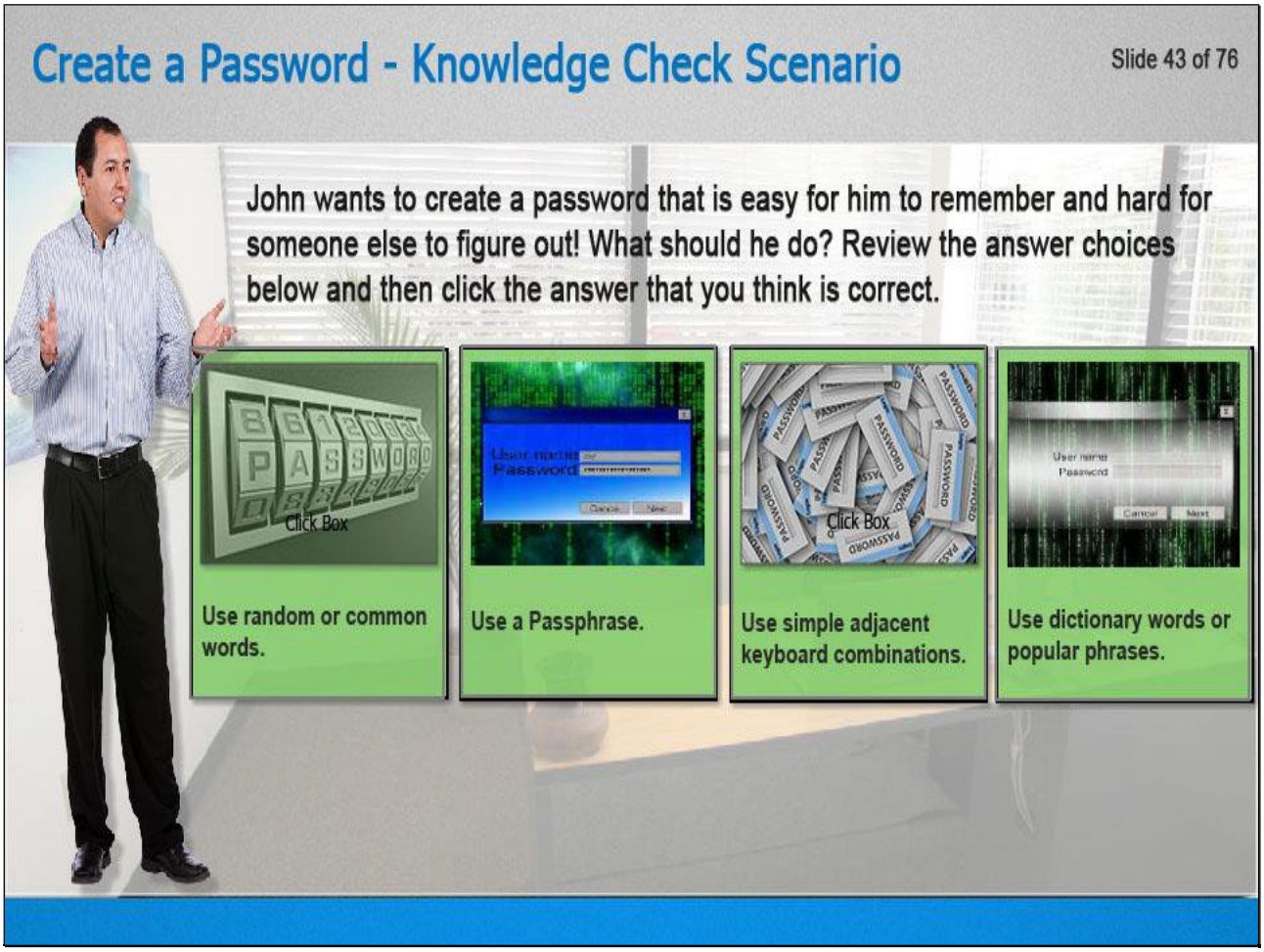
Staff should not use words included in a dictionary or popular phrases. System intruders may try to use special tools called "password crackers" that include all dictionary words, and it can be modified to include popular phrases and sports teams to guess your password.

Please take a moment to review the examples given regarding password combinations that you should never use.

Password Best Practices, cont.



Create a Password - Knowledge Check

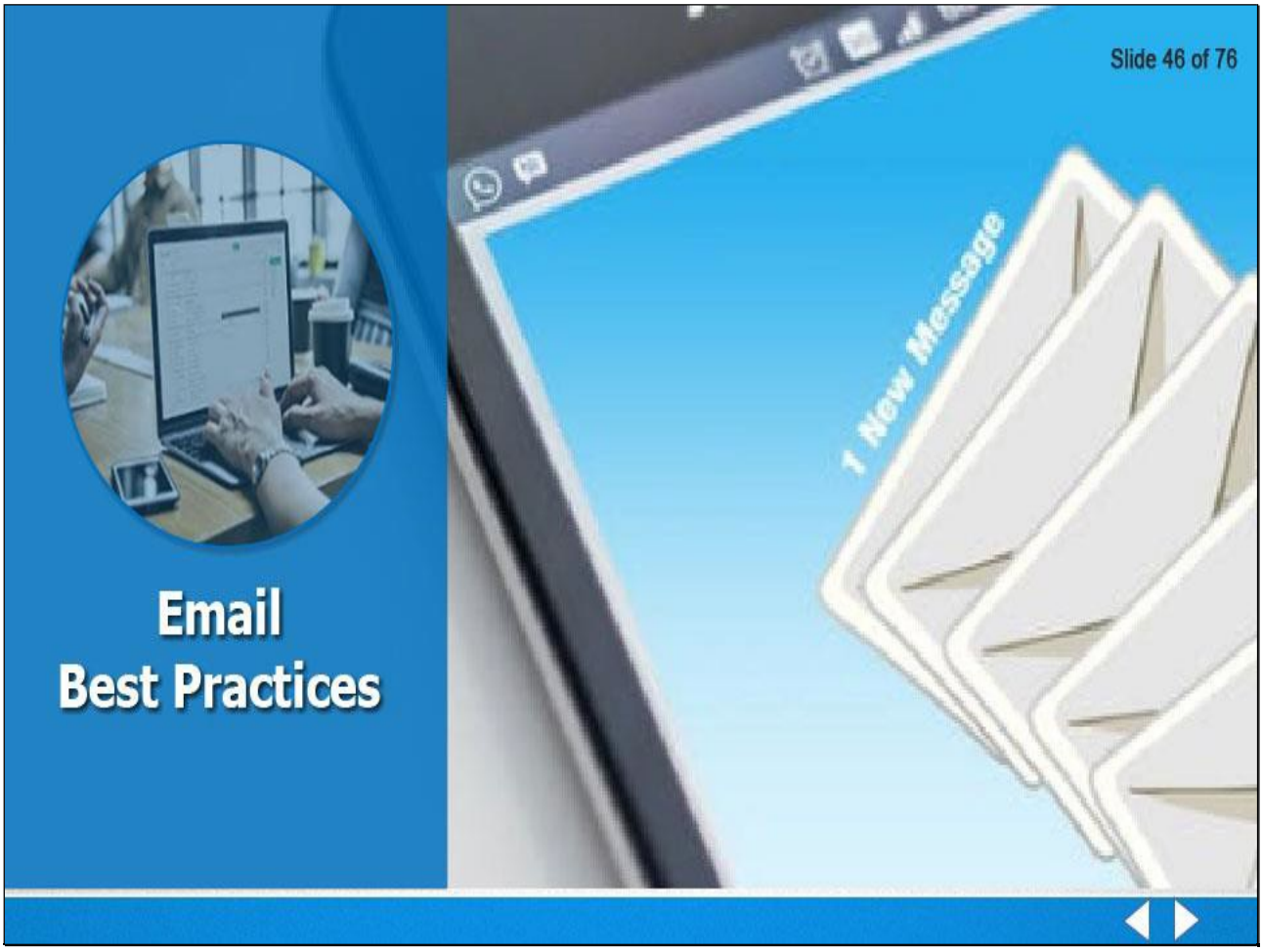


Notes

John wants to create a password that is easy for him to remember and hard for someone else to figure out!

What should he do: Using a passphrase is one of the most secure types of passwords you can create. A passphrase is easy to remember but hard for others to guess.

Email Best Practices



Notes

Now that we have explained the security responsibilities of all Revenue staff, let's discuss some best practices for email.

The next slide includes a video transcript on external threats.

External Threats

Video Transcript

Outside threats are primarily going to come from bad guys trying to get in mostly through email or other methods that most staff wouldn't be aware of that IT or security protects us from.

External threats typically are going to be from criminals looking for money or access to data that could be states or foreign countries trying to access our systems, to disrupt our economy, or it could just be a casual kid that's gotten some software at college and decides they want to poke at it to see if they can get in.

You should never respond to SPAM

Notes

It is important that all personnel understand the risks associated with responding to Spam. Here are few reasons why you should NEVER respond to Spam. Responding to Spam will, let the Spammer know your account is active, then they can pass your information onto other spammers, which will cause a great increase in the amount of spam you receive.

You should note: clicking the “Unsubscribe” link is also considered responding. Responding will, allow the Spammer to potentially coax you into giving him or her sensitive information.

Due to the fact that spam emails often bear fake source email addresses, by responding you may unwillingly collaborate in a devious scheme meant to saturate the mailbox of some unsuspecting target victim. If you believe you have received a spam message, you should always report it to the Service Desk.

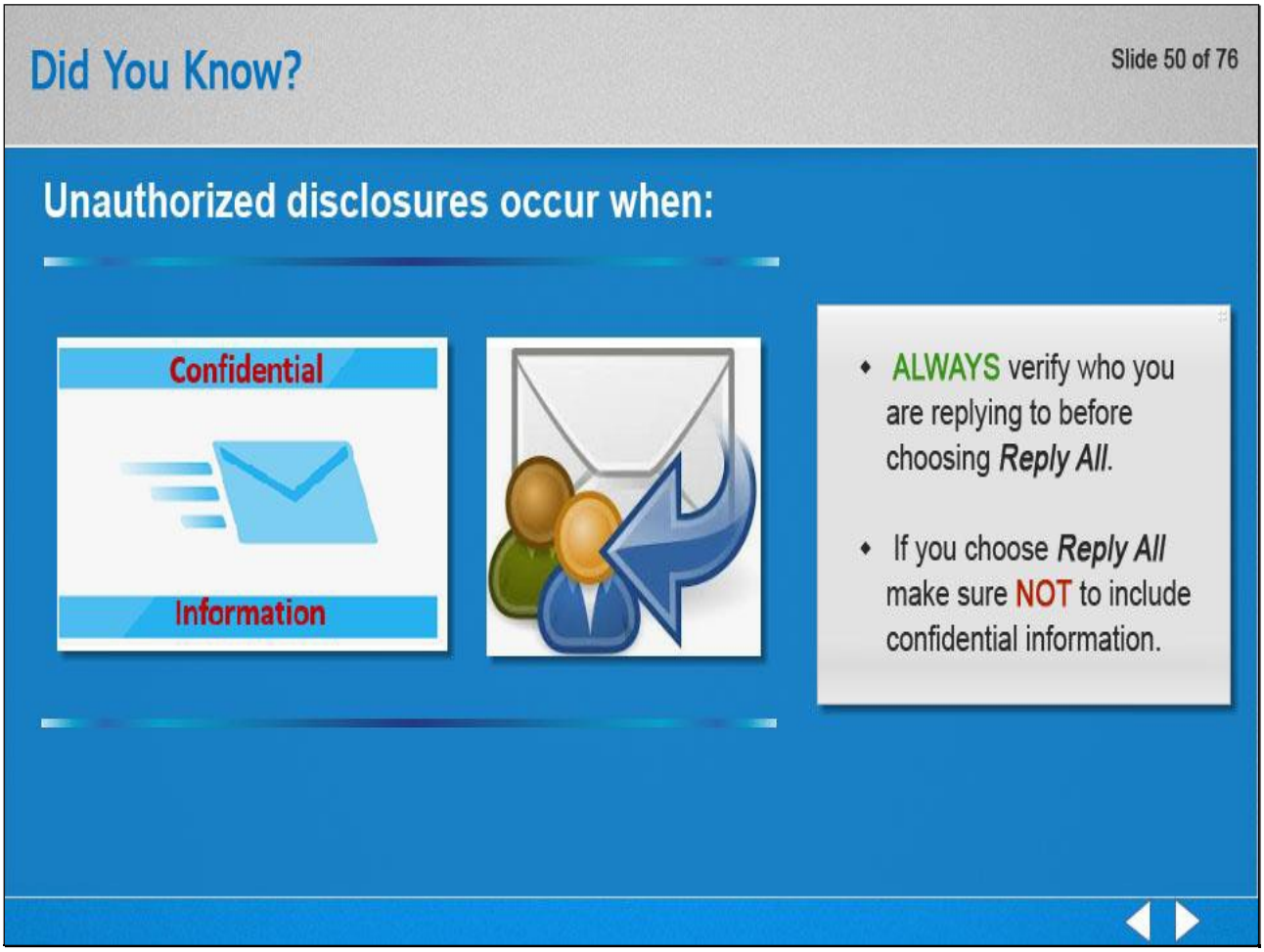
Let’s review how to report it next.

SPAM Email

If you receive an email that you suspect is spam, you must send it to the Service Desk in the following manner:

1. Click **New Email**.
2. Enter the **Service Desk email address** in the To field (ServiceDesk@ncdor.gov)
3. **Attach the SPAM email** to the new email by selecting **Insert → Outlook Item**.
4. In the pop-up window, **select the SPAM message(s)**.
5. Click **OK**.
6. Click **Send** to send the message to the Service Desk.

Did You Know?



Notes

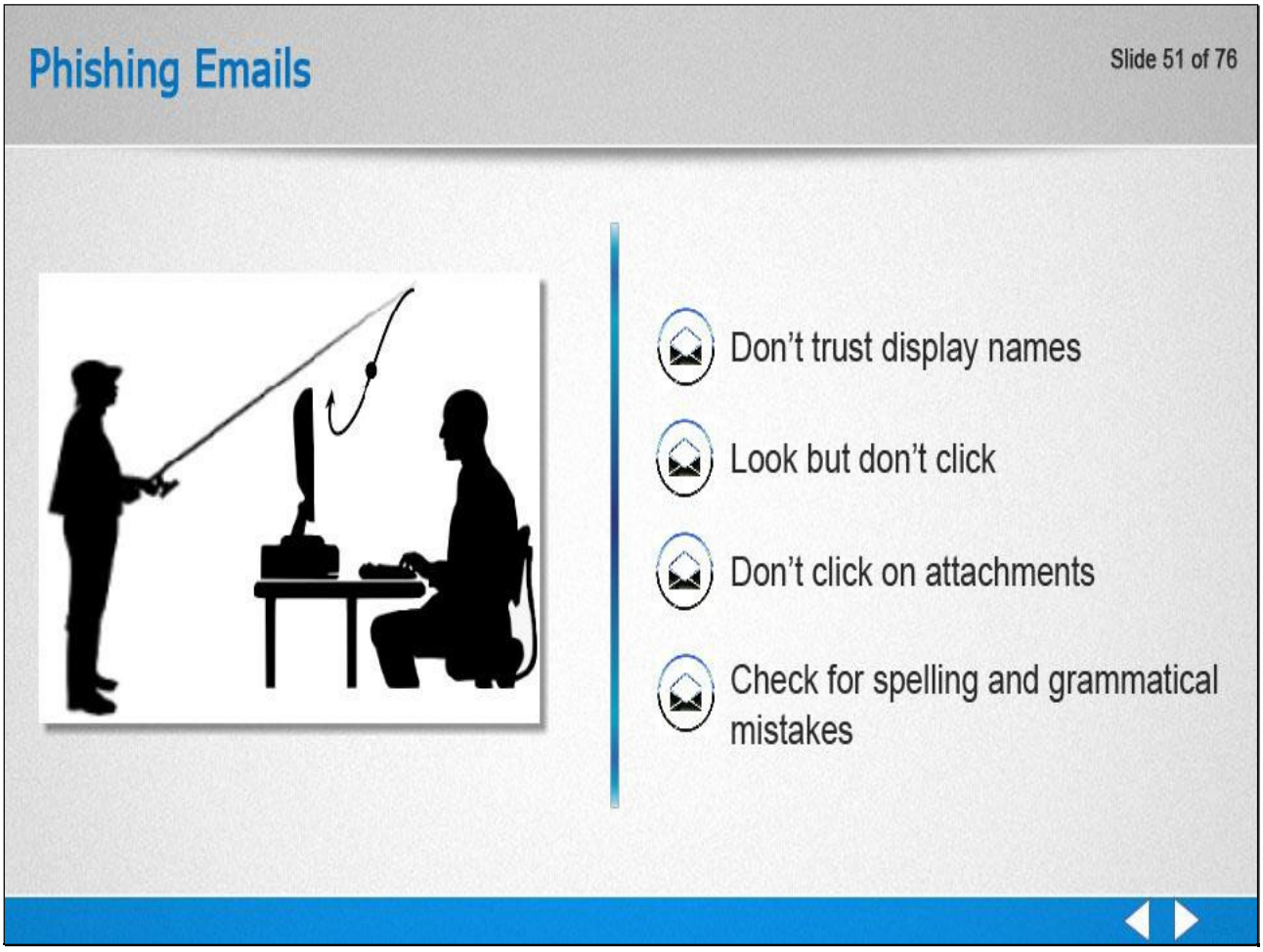
One of the most common ways “unauthorized disclosures” occur is when personnel insert confidential information (into an email) and then choose Reply All without first checking exactly who the email is going to.

It is always a good idea to check your email at least twice before hitting the send button to ensure that you have reviewed what information you are sending out and who you are sending it to.

To avoid this, always verify who you are replying to before choosing Reply All.

If you choose Reply all make sure NOT to include confidential information.

Phishing Emails



Notes

Phishing emails are getting more sophisticated every day.

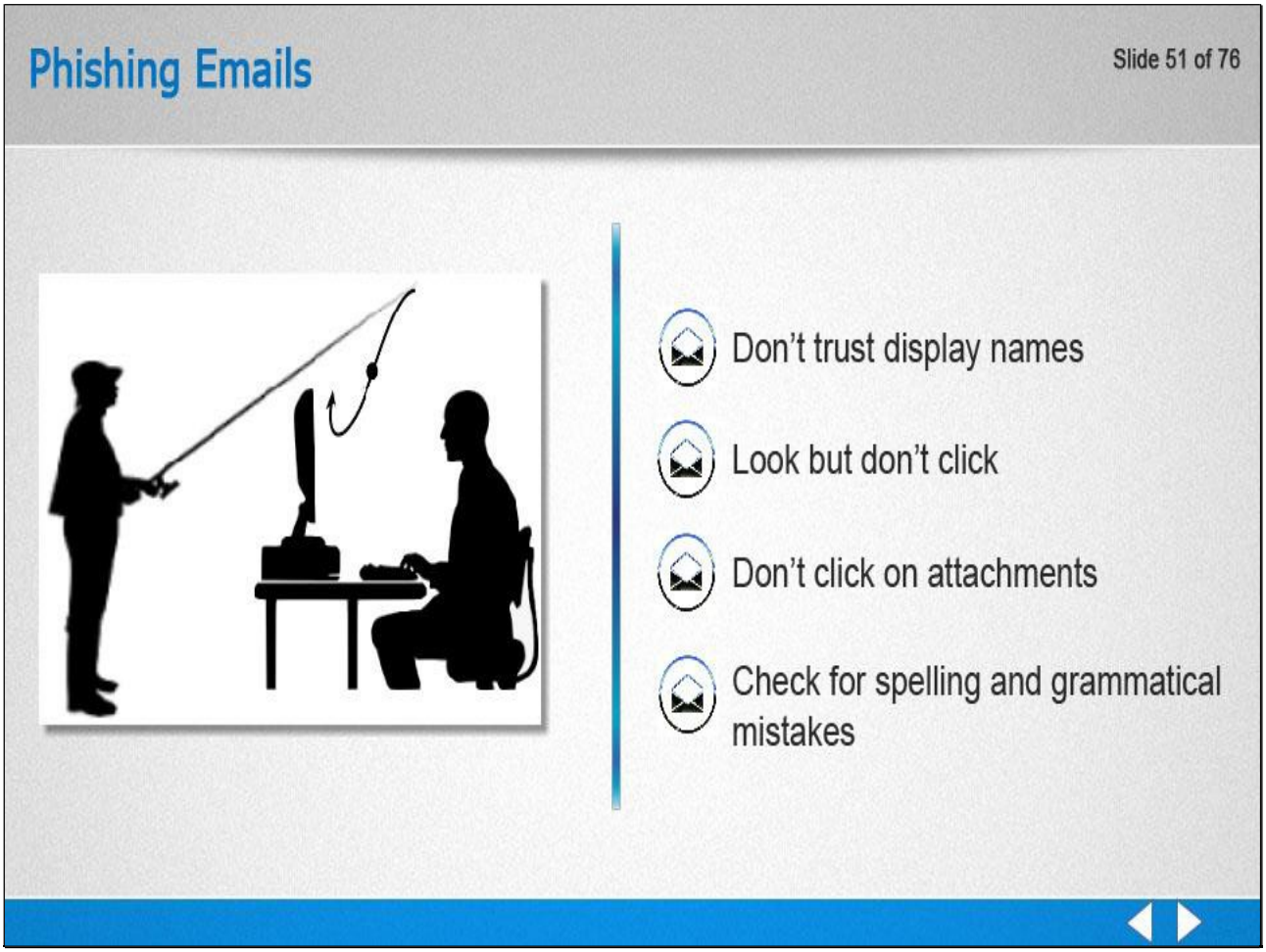
With some scrutiny, you can spot a phishing email using a few techniques.

Don't trust display names: These can be easily faked. Always check the email address in the from field, if it looks suspicious, don't open it. Ensure that you are seeing the sender's email address and evaluate it well.

Look but don't click. The text of the link is easily editable by the person creating the link.

By hovering the mouse over the link essentially moving the mouse arrow over the link but not clicking on it, you can see the actual destination of where the link is trying to send you. If it looks suspicious, do not click it.

Phishing Emails, cont.



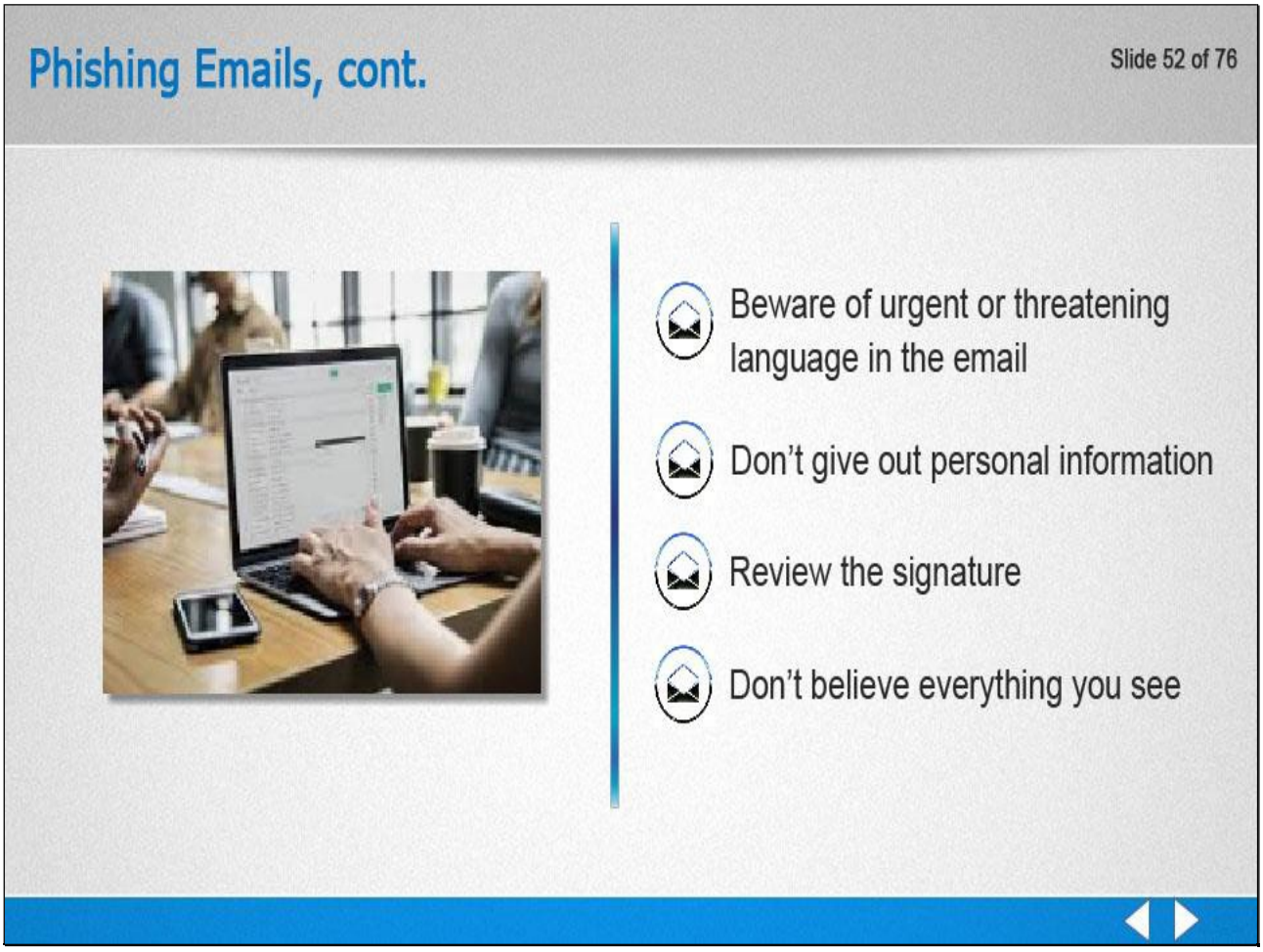
Notes, cont.

Don't click on attachments: Including malicious attachments that contain viruses and malware have become a very common phishing tactic. Malware can damage files on your computer, steal your passwords, or spy on you without your knowledge.

Attachments have embedded code that can be executed when the attachment is opened. Do not open any email attachments you were not expecting. Not always but many times a quick phone call to the sender can help to determine if an attachment is malicious or safe. If you are not expecting the attachment, do not open it.

Check for spelling and grammatical mistakes: Another way to identify phishing email is to check the grammar of the email. Especially if the email is from a business. This could be a sign that something is not right. Legitimate messages usually do not have major spelling mistakes or poor grammar. Always read through your emails carefully.

Phishing Emails, cont.



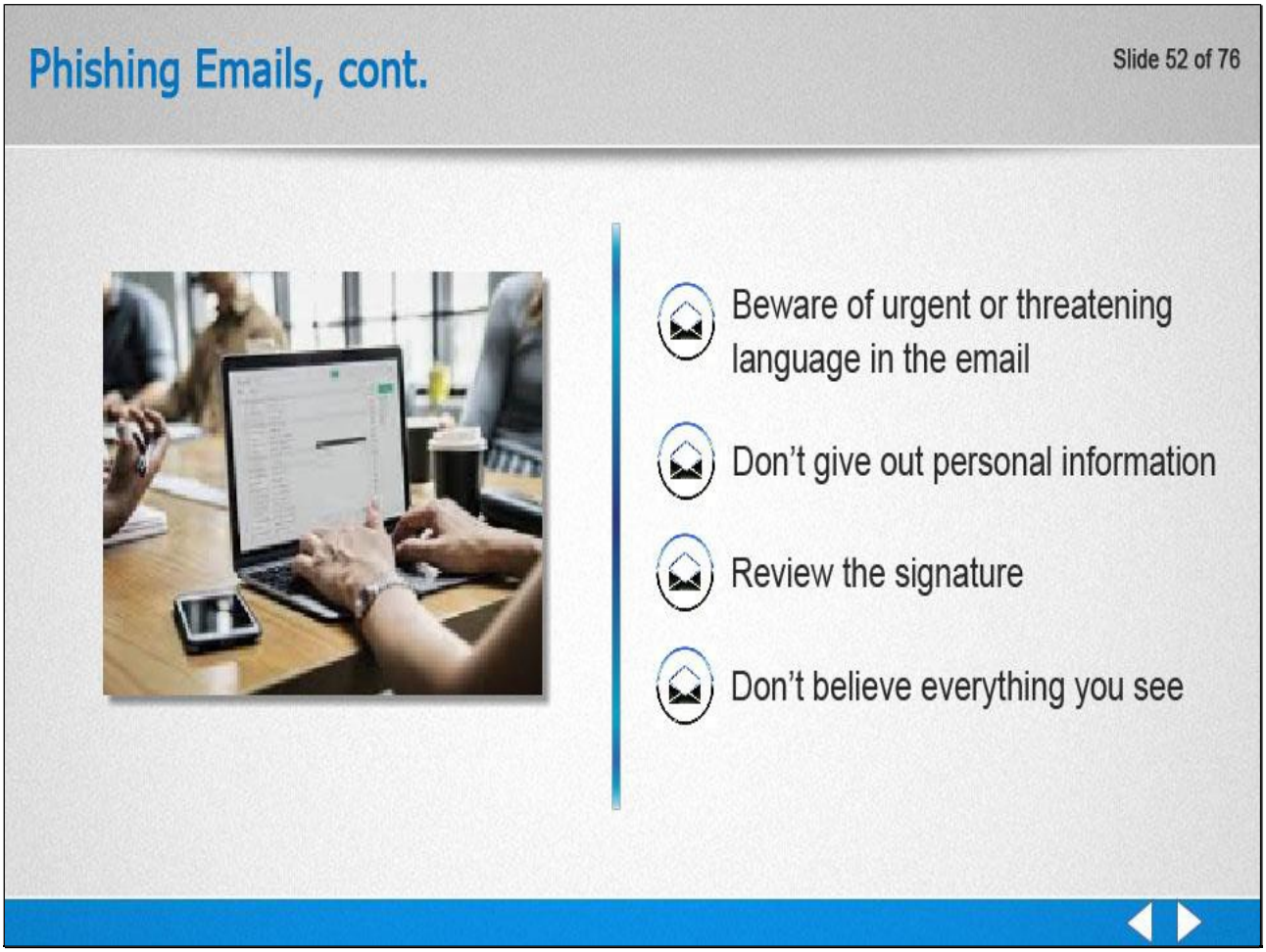
Notes

Beware of urgent or threatening language in the email: Invoking a sense of urgency or fear is a common phishing tactic. Attackers want you to open the email and click on links and they will try to use tricks like these to do just that. Beware of subject lines that claim your "account has been suspended" or your account had an unauthorized login attempt.

Don't give out personal information. Legitimate banks and most other companies will never ask for personal credentials through email. So do not give them out.

Review the signature: When trying to determine if the email is a phishing email, you should always look at the signature. If there is a lack of information about the sender or ways to contact the sender, you may want to evaluate the email more to see if there are any other signs that this is a phishing email. Lack of details about the sender or how you can contact a company strongly suggests it is a Phish. Legitimate businesses always provide contact details.

Phishing Emails, cont.



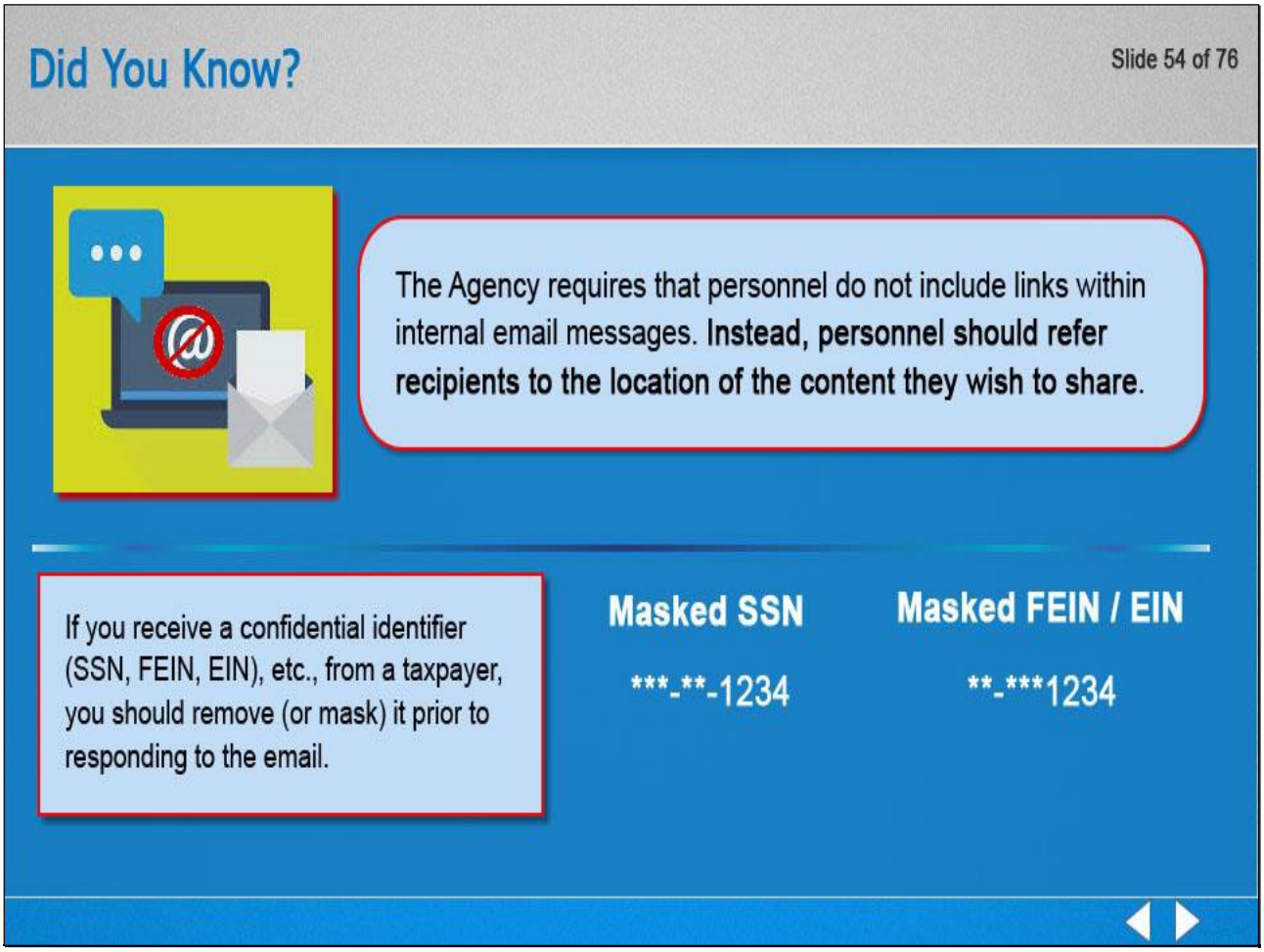
Notes, cont.

Don't believe everything you see: Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it is legitimate. Logos and images are easy to copy and paste. Email addresses are easy to create.

Always trust your instinct. It is always better to err on the side of caution.

Be skeptical when it comes to your email messages. If it looks even remotely suspicious, don't open it.

Did You Know?



Notes

The agency requires that personnel do not include links within internal email messages. What does this mean for you? If you receive an email which includes a link - do not click it! You must report the suspicious message to the Service Desk.

If you receive a confidential identifier (SSN, FEIN, EIN), etc., from a taxpayer, you should remove (or mask) it prior to responding to the email.

Staff should not include full identifiers within email because all email transmissions are considered public record. Not including full identifiers mitigates the risk of potential unauthorized disclosures in the future.

Review the examples provided on the slide of a masked Social Security Number and Federal Employee Identification Number and Employee Identification Number.

Security Measures that employees should follow

Video Transcript

Primary things that employees need to watch out for on what you're doing on a day-to-day basis is basically, be aware.

We kind of get complacent from day-to-day on what's going on and we forget to do certain things. We get in a routine, right.

A couple things that are pretty straightforward is to watch for badges. It's very easy for somebody especially when we're crowded, or in and out for lunch. For example, a bad guy can basically get behind you and surf through the gates that we have downstairs and at the elevator, just check and make sure people are wearing their badges. It's not rude for you to say "Hey, where's your badge." That's part of the security requirements here at DOR and something that we need to watch for.

Mail, don't click stuff, don't open stuff, I've said that repeatedly. I think I beat everybody to death with that. It is extremely important as I said 98% percent of breaches come that way. We have systems in place to try to protect from that. But it's still very important that you're aware of whose sending you attachments, files, and links. If you don't know who they are, don't click it. Reach back out, let IT know, call the help desk.

Facility Security Policy Reminders

Video Transcript

Now that we have explained some email best practices, let's discuss a few facility security reminders.

Here are some reminders about facility security policies:

- You should always wear your badge between the neck and waist.
- This allows all staff including those who are responsible for the security of our building know who you are and that you are NCDOR staff.
- Always report a lost or stolen badge immediately to the service desk, security guard, or Director of Business Operations.
- Personnel should never share their badge with anyone.
- NCDOR visitors must be escorted at all times.
- Personnel should never allow another individual to piggyback or tailgate through security checkpoints, e.g. doors with badge access.

Alternative Worksites

Notes

There may be situations where staff need to use or access Revenue information while away from a Revenue facility. These locations are considered alternative work sites.

Some examples of acceptable work sites may include:

- a customer's tax office
- an employee's hotel room during official business travel; or
- a teleworker's home office

Even though staff may be conducting official business with a customer, staff is reminded to refrain from accessing or discussing Revenue business in public areas, such as airports or coffee shops.

Alternative Worksites, cont.

Notes, cont.

Discussing Revenue information in these types of locations may put staff at risk of making an unauthorized disclosure of confidential information.

Alternative Worksites, cont.

Notes

It should also be remembered that the same security safeguards are required when handling confidential information at alternative work sites as you do when working within a Revenue facility.

Some examples include:

- Adhere to the agency's clean desk policy,
- Be aware of your conversation level as not to be overheard by others,
- Update your voice message to inform taxpayers not to leave Personal Identifiable Information,
- Forward business calls to your Revenue issued cellular phone that requires a PIN to retrieve messages,
- And, Do not leave confidential information on any unattended computers

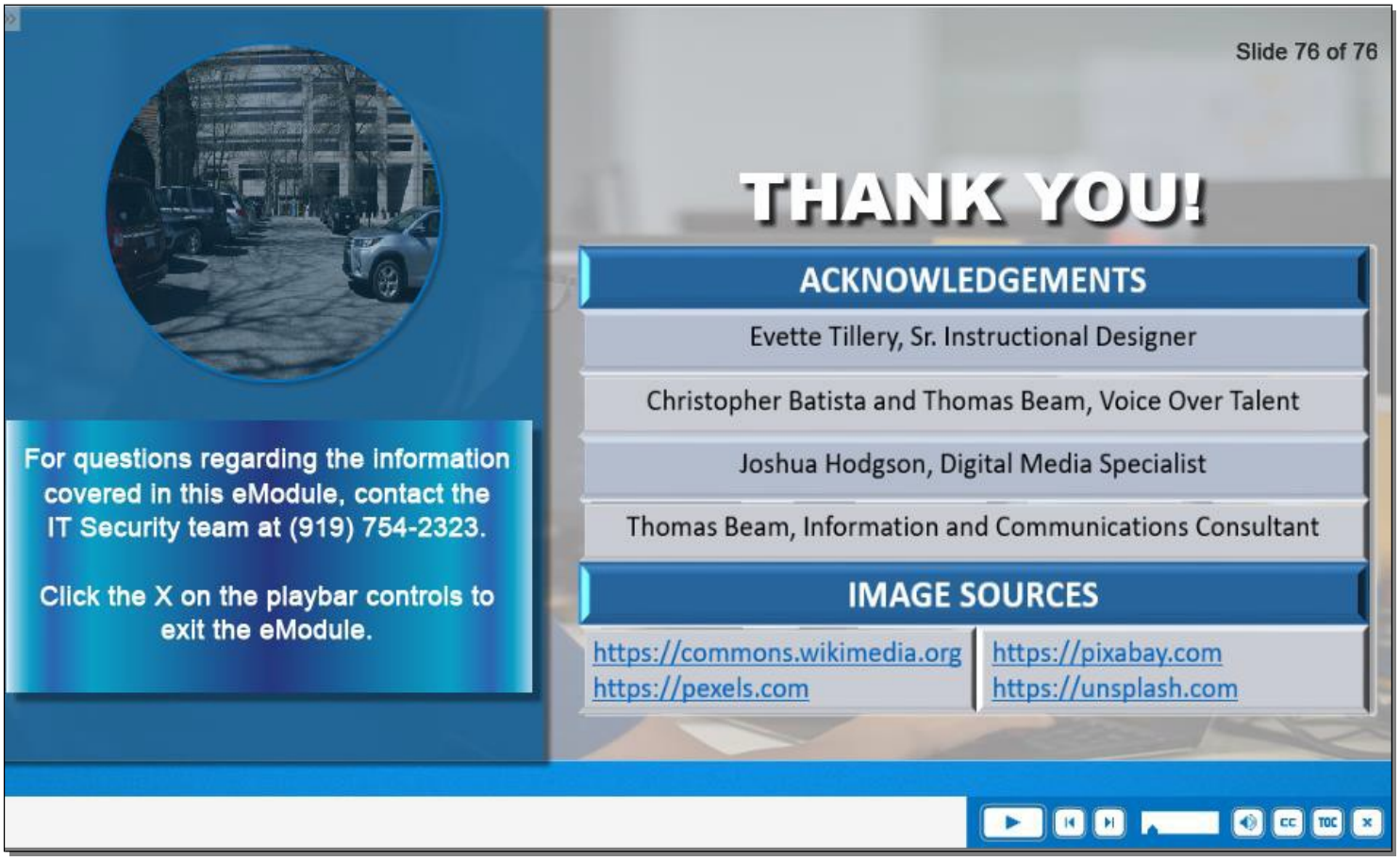
Alternative Worksites, cont.

It should also be remembered that the same security safeguards are required when handling confidential information at alternative work sites as you do when working within a Revenue facility.

Some examples include:

- Adhere to the agency's clean desk policy,
- Be aware of your conversation level as not to be overheard by others,
- Update your voice message to inform taxpayers not to leave Personal Identifiable Information,
- Forward business calls to your Revenue issued cellular phone that requires a PIN to retrieve messages,
- And, Do not leave confidential information on any unattended computers

Thank You!



Notes

You have reached the end of the 2019 Information Security and Privacy Awareness Training.

If you have questions regarding the information covered in this training eModule, contact the IT Security team at 919-754-2323.