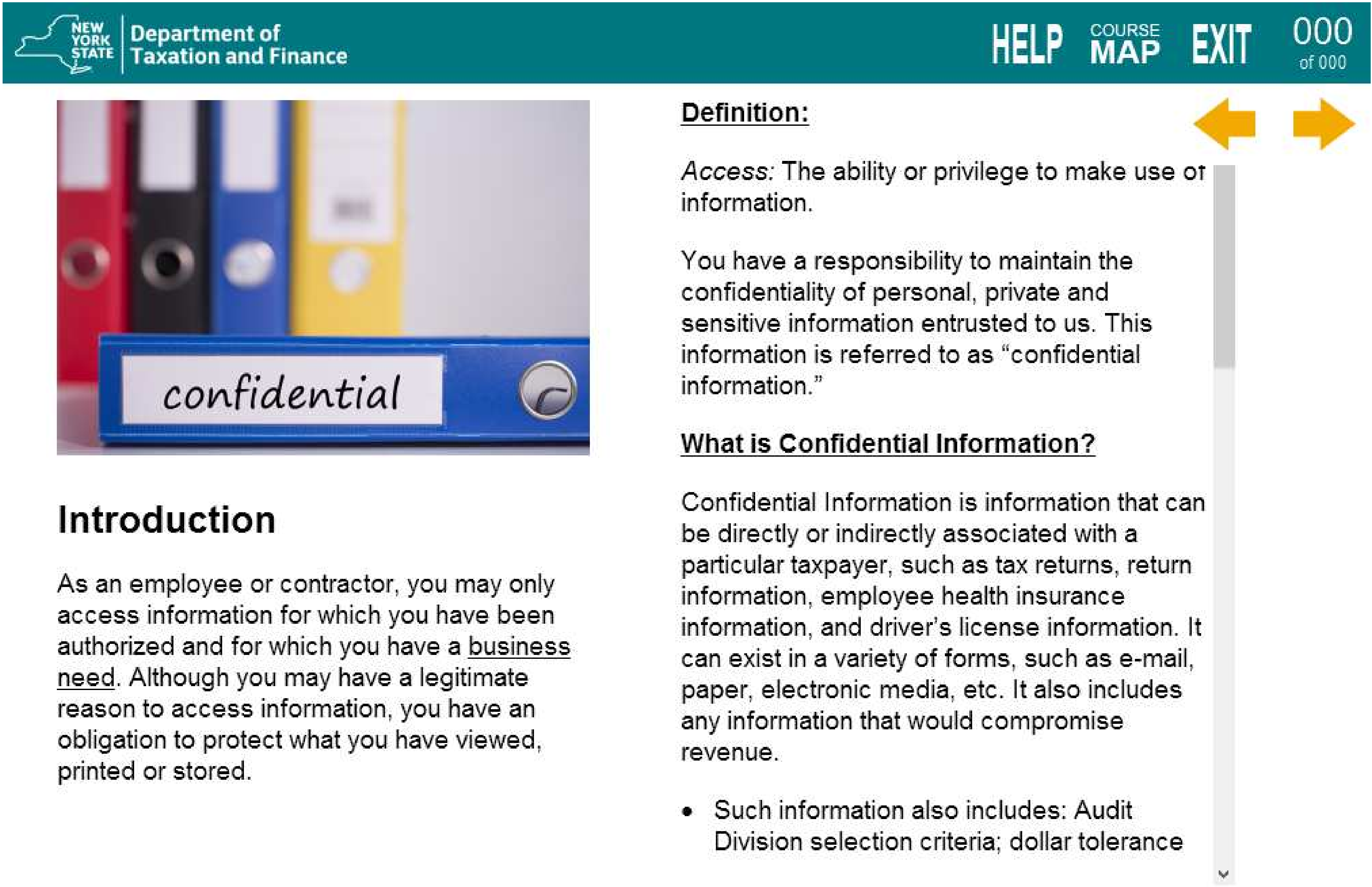
Department of Taxation and Finance

2017 Annual Access and Disclosure Training for Non-DTF Employees

Get Started ▶



Introduction

As an employee or contractor, you may only access information for which you have been authorized and for which you have a <u>business need</u>. Although you may have a legitimate reason to access information, you have an obligation to protect what you have viewed, printed or stored.

<u>Definition:</u>

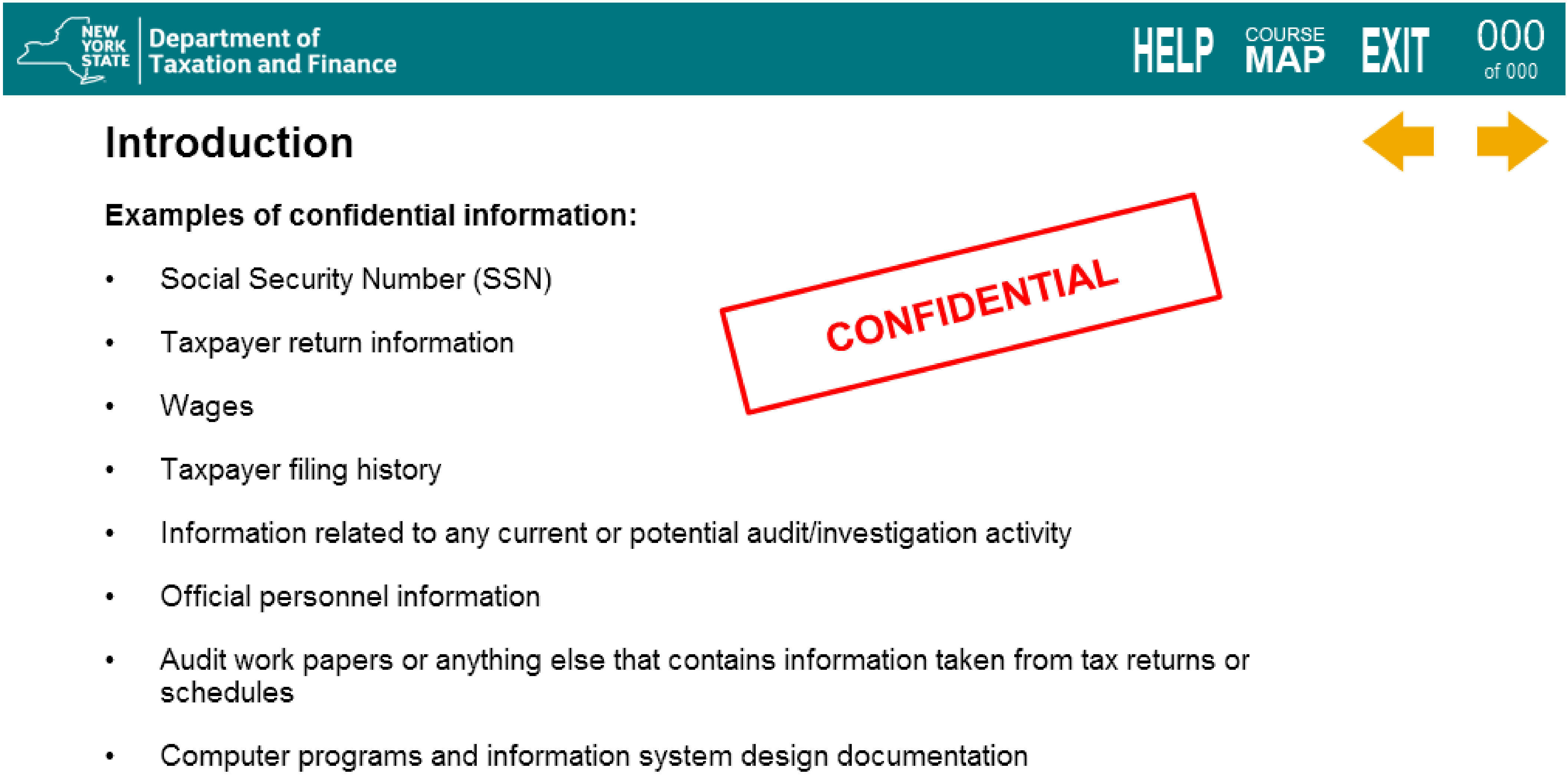
Access: The ability or privilege to make use of information.

You have a responsibility to maintain the confidentiality of personal, private and sensitive information entrusted to us. This information is referred to as “confidential information.”

<u>What is Confidential Information?</u>

Confidential Information is information that can be directly or indirectly associated with a particular taxpayer, such as tax returns, return information, employee health insurance information, and driver’s license information. It can exist in a variety of forms, such as e-mail, paper, electronic media, etc. It also includes any information that would compromise revenue.

- Such information also includes: Audit Division selection criteria; dollar tolerance



Introduction

Examples of confidential information:

- Social Security Number (SSN)
- Taxpayer return information
- Wages
- Taxpayer filing history
- Information related to any current or potential audit/investigation activity
- Official personnel information
- Audit work papers or anything else that contains information taken from tax returns or schedules
- Computer programs and information system design documentation

Introduction

Need to Know

Accessing confidential information must be limited to what you "need to know" in order to perform your official responsibilities. **Official duties <u>NEVER</u> include** accessing your own tax records or those of co-workers, neighbors, friends or family. You are **NOT** allowed to access your own tax records or those of co-workers, neighbors, friends or family for training, testing, or other work-related programming activities.

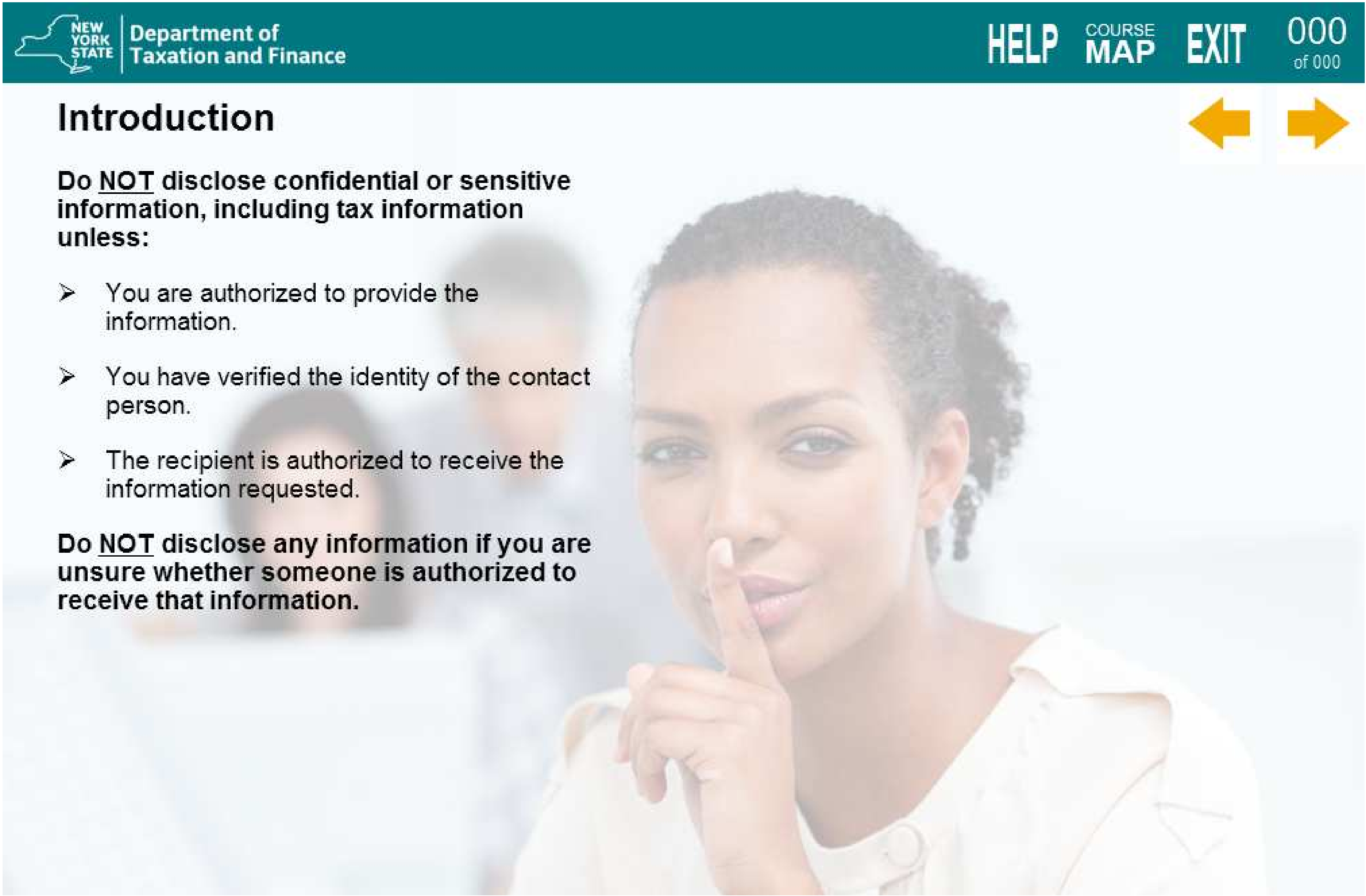
Without the "need to know," you are not authorized to access, attempt to access, request or modify confidential information.

Introduction

Confidential information **CANNOT** be disclosed or shared with others unless they are properly authorized and have a “need to know.” By completing this training you are not only acknowledging your understanding of these concepts, you are also declaring your personal commitment to maintaining the confidentiality and privacy of taxpayer information.

Definition:

Disclosure: Making information known in any manner, including phone calls, faxes, letters, discussions or any electronic means, such as e-mail. This includes disclosures to yourself of information you are not entitled to know.

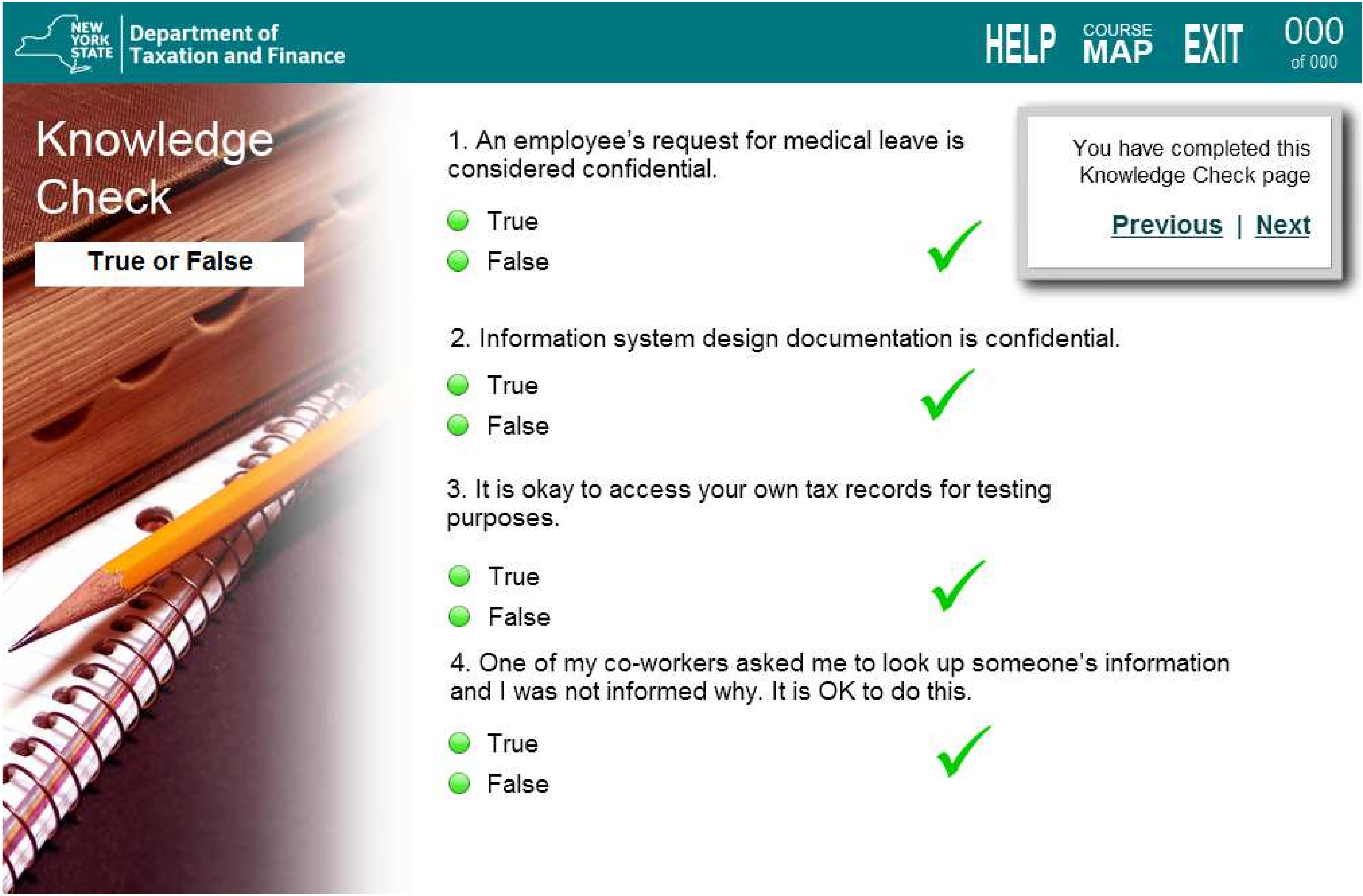


Introduction

Do NOT disclose confidential or sensitive information, including tax information unless:

- You are authorized to provide the information.
- You have verified the identity of the contact person.
- The recipient is authorized to receive the information requested.

Do NOT disclose any information if you are unsure whether someone is authorized to receive that information.



Knowledge Check

True or False

1. An employee's request for medical leave is considered confidential.

● True
● False ✓

You have completed this Knowledge Check page

Previous | Next

2. Information system design documentation is confidential.

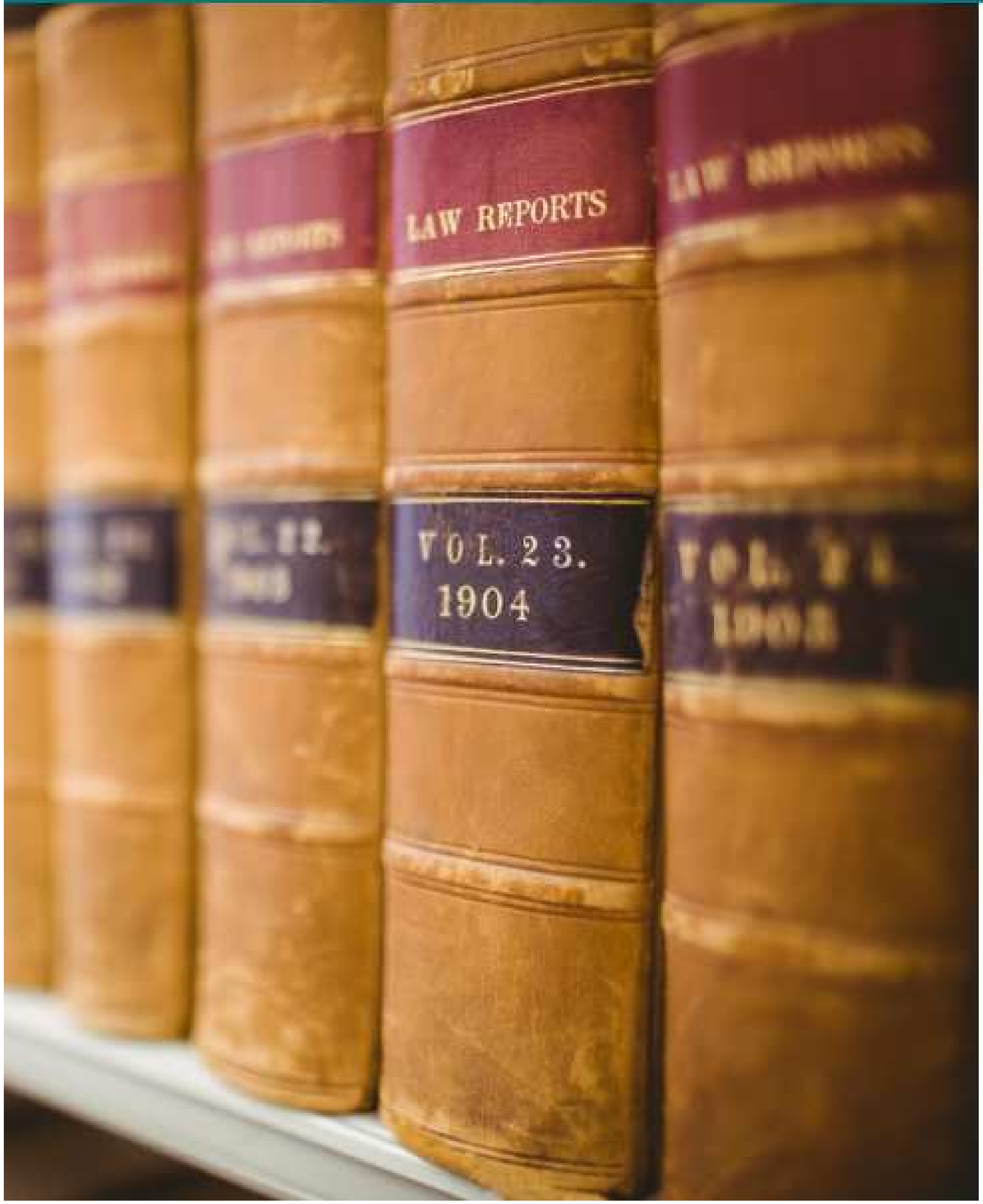
● True ✓
● False

3. It is okay to access your own tax records for testing purposes.

● True ✓
● False

4. One of my co-workers asked me to look up someone's information and I was not informed why. It is OK to do this.

● True ✓
● False



Public Officers Law

Section 73 and Section 74 of the Public Officers Law provides standards of conduct and ethics of all state officers, employees and party officers.

Computer Security

Every time you access our confidential computer systems, you are reminded about the penalties and possible disciplinary actions for unauthorized access, disclosure or use of confidential information. When accessing our computer systems, you are subject to routine monitoring of account activities for improper use.

Computer Security

Password Rules:

Each person is responsible for any activity that takes place under his/her USER ID. Following the PASSWORD guidelines below, will help secure all activity performed under your USER ID.

Password Guidelines:

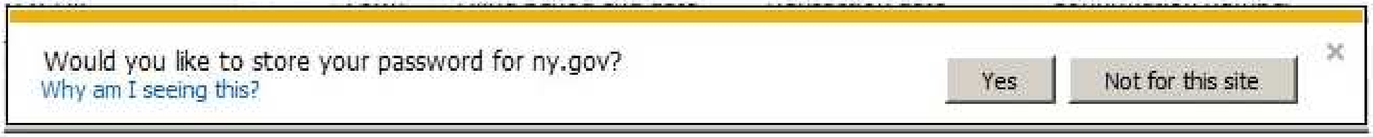
- Use PASSWORDS that CANNOT be easily guessed.
- Never let anyone use your USER ID or PASSWORD to log in.
- Never share your PASSWORD with anyone, not even your supervisor or Help Desk Staff.
- Do NOT write your PASSWORD down.
- Do NOT use the same PASSWORD for different systems (e.g. home PC, personal e-mail account, personal bank account, etc…)

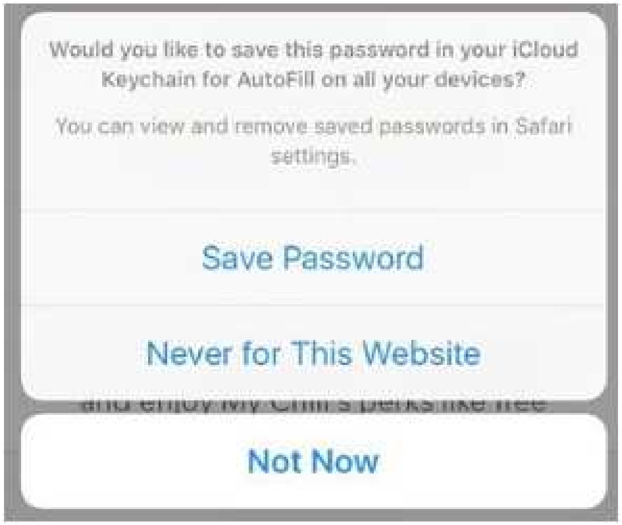
Computer Security

Password Retention Pop-up

You may see one of the following messages below when a password is required to perform job functions such as accessing NY.GOV:

- ➢ **DO NOT** click “Yes” or "Save Password"
- ➢ **DO CLICK** “No,” “Not for this site,” or “Never for This Website"


Would you like to store your password for ny.gov?
Why am I seeing this?


Would you like to save this password in your iCloud Keychain for AutoFill on all your devices?

You can view and remove saved passwords in Safari settings.

Computer Security

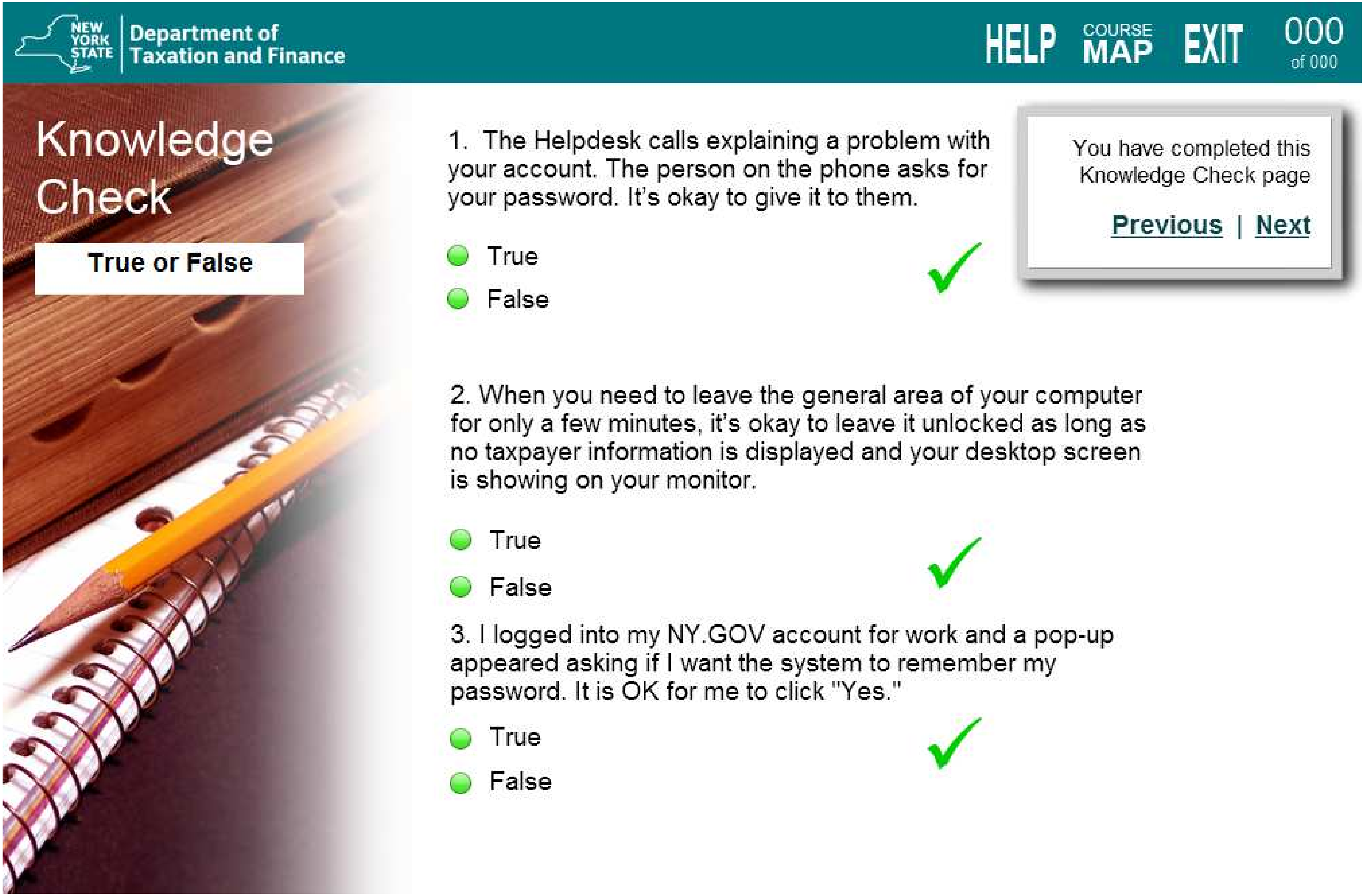
Security Guidelines for DTF Computer Use:

Always log off, lock up (Ctrl, Alt & Delete) or shut down your computer whenever you are away from it.

- Locking your computer can be done by pressing Ctrl, Alt & Delete, then click on “Lock this computer” or simply click the Windows Key & L. If using a virtual machine, press Ctrl, Alt & Insert, then click on “Lock this computer.”

Be aware of others around you when looking at confidential information.

DO NOT install unauthorized files or software on your computer.



Knowledge Check

True or False

1. The Helpdesk calls explaining a problem with your account. The person on the phone asks for your password. It's okay to give it to them.

● True

● False ✓

You have completed this Knowledge Check page

Previous | Next

2. When you need to leave the general area of your computer for only a few minutes, it's okay to leave it unlocked as long as no taxpayer information is displayed and your desktop screen is showing on your monitor.

● True

● False ✓

3. I logged into my NY.GOV account for work and a pop-up appeared asking if I want the system to remember my password. It is OK for me to click "Yes."

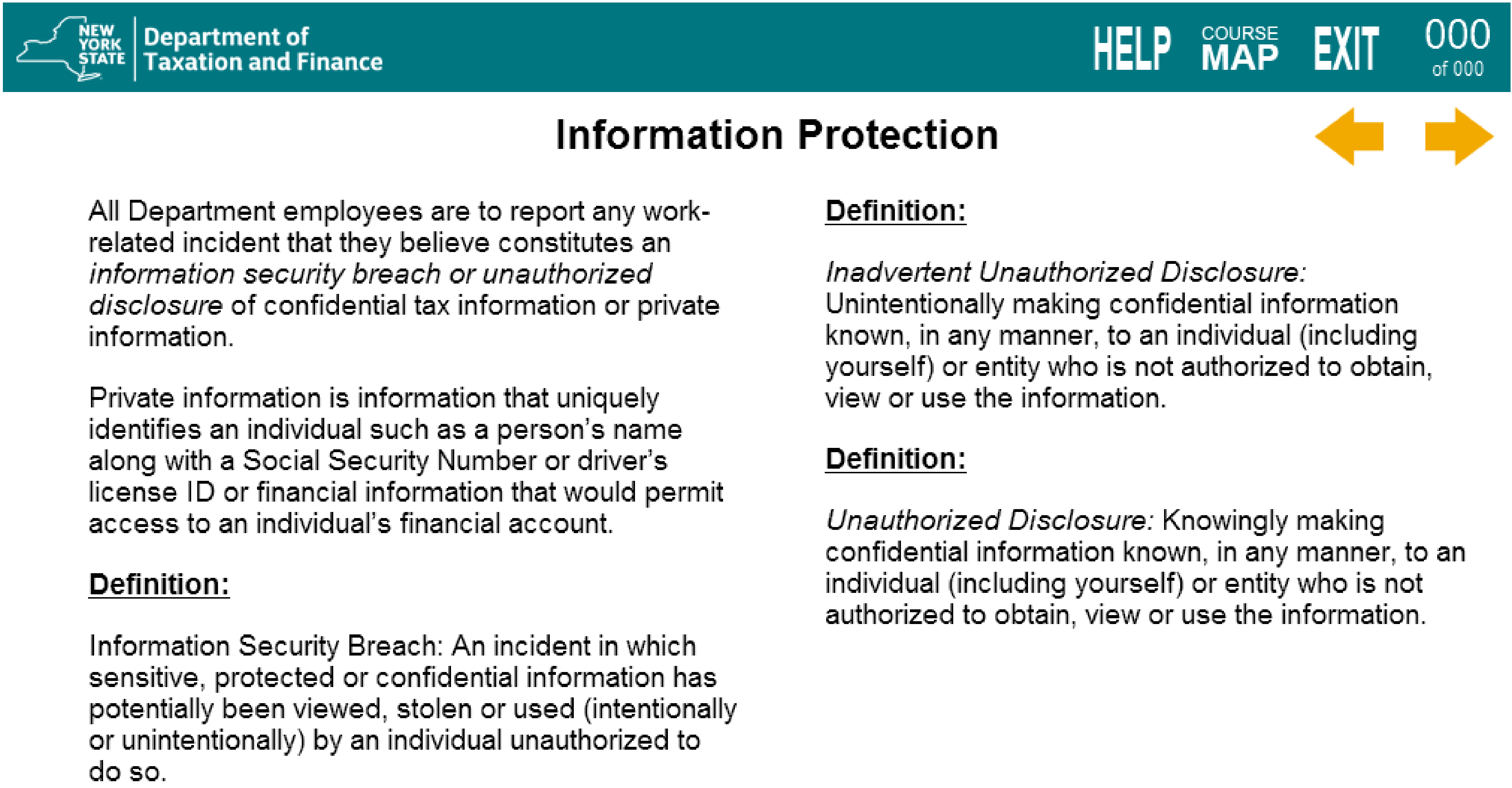
● True

● False ✓

Information Protection

The New York State Information Security Breach and Notification Act requires New York State entities to contact affected persons, without unreasonable delay, after any breach of security, unauthorized access or unauthorized release of computerized private data.

Additionally, the Department has enhanced its reporting requirements to also include hard-copy confidential documents.



Information Protection

All Department employees are to report any work-related incident that they believe constitutes an *information security breach or unauthorized disclosure* of confidential tax information or private information.

Private information is information that uniquely identifies an individual such as a person's name along with a Social Security Number or driver's license ID or financial information that would permit access to an individual's financial account.

Definition:

Information Security Breach: An incident in which sensitive, protected or confidential information has potentially been viewed, stolen or used (intentionally or unintentionally) by an individual unauthorized to do so.

Definition:

Inadvertent Unauthorized Disclosure: Unintentionally making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.

Definition:

Unauthorized Disclosure: Knowingly making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.

Information Protection

Examples of an Unauthorized Disclosure would include:

Inadvertent Unauthorized Disclosure

Some examples are:

- Mail or faxes sent to the wrong party.
- A briefcase containing taxpayer information was left unsupervised and its location cannot be determined.
- Documents containing Federal Tax Information (FTI) cannot be located.

Unauthorized Disclosure

Some examples are:

- An employee accesses his daughter's tax return and shares it with her.
- An employee shares with friends the tolerance amounts that Audit has established for issuing bills.

All of the above would be considered an Information Security Breach.

Information Protection

Reporting Requirements

ITS staff and ITS contractors:

- Immediately report any suspected inappropriate activity, unauthorized access, unauthorized disclosure, or any other suspected breaches to your appropriate manager and the Information Security Officer (ISO)/designated security representative.
- Follow the reporting procedures found on the NYS ITS EISO incident link – http://its.ny.gov/incident-reporting

Everyone else:

To report an unintentional information security breach, immediately contact the DTF Information Security Office

To report any inappropriate activity (such as unauthorized access or disclosure), immediately contact the DTF Office of Internal Affairs (518) 451-1566.

Information Protection

Properly Dispose of Confidential Information:

You must shred confidential paper documents using a Department approved shredder, or you may place them in a locked confidential destruction bin where available. Do **NOT** place any papers containing confidential information in the trash, recycling (3R's) baskets or in open gondolas.

You must properly dispose of all electronic portable media, such as diskettes, CDs, DVDs, flash drives, computer tapes, optical disks, hard drives, removable drives of any kind, or any other USB connected storage media that contains confidential information.

*Please refer to the Disposal of Electronic Media Policies and Procedures to view the policies and procedures for the secure handling and disposal of confidential information.

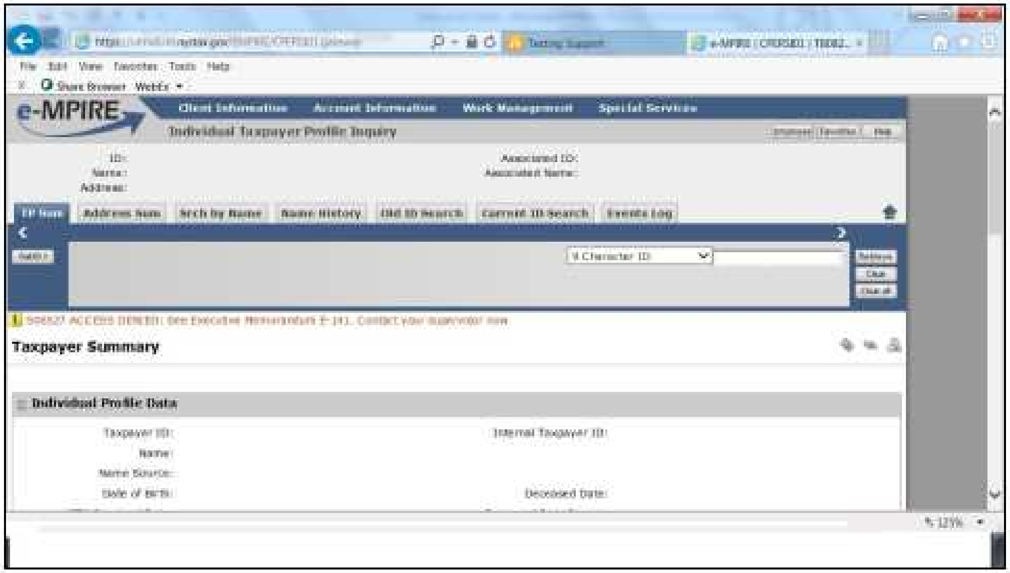
***Please direct any questions on electronic media disposal to OSB at tax.sm.OSB.Support.Services.**

"Access Denied" Error Message

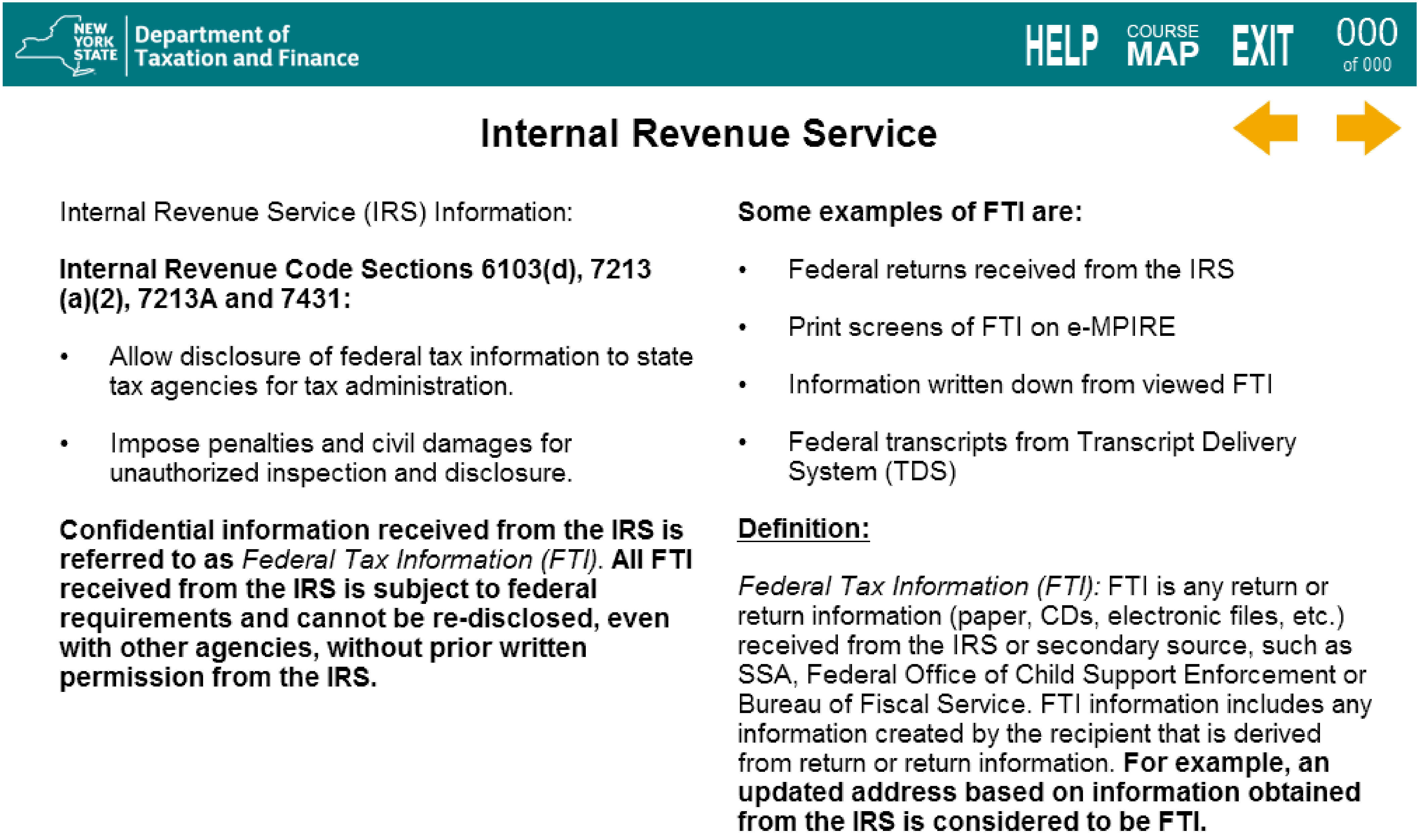
The Department prevents persons with access to e-MPIRE from accessing certain records which are flagged as being associated with the user and therefore are inaccessible. There are a variety of reasons for an account to be flagged, for example, a spouse listed on a primary return for the employee who now files returns independently.

When an employee goes to e-MPIRE and enters information to look at one of these accounts, they will receive a message that looks like this.

This message may also be generated from work that is randomly pushed to an employee through automated workflow processes. If you receive this message you must immediately notify your supervisor to document the reason you were attempting to access that account.



S06527 ACCESS DENIED: See Executive Memorandum E-141. Contact your supervisor now



Internal Revenue Service

Internal Revenue Service (IRS) Information:

Internal Revenue Code Sections 6103(d), 7213 (a)(2), 7213A and 7431:

- Allow disclosure of federal tax information to state tax agencies for tax administration.
- Impose penalties and civil damages for unauthorized inspection and disclosure.

Confidential information received from the IRS is referred to as *Federal Tax Information (FTI).* **All FTI received from the IRS is subject to federal requirements and cannot be re-disclosed, even with other agencies, without prior written permission from the IRS.**

Some examples of FTI are:

- Federal returns received from the IRS
- Print screens of FTI on e-MPIRE
- Information written down from viewed FTI
- Federal transcripts from Transcript Delivery System (TDS)

Definition:

Federal Tax Information (FTI): FTI is any return or return information (paper, CDs, electronic files, etc.) received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI information includes any information created by the recipient that is derived from return or return information. **For example, an updated address based on information obtained from the IRS is considered to be FTI.**

Internal Revenue Service

(IRS) Information, continued…

The IRS requires that FTI be tracked from the time it is received to the time it is destroyed.

- Whenever employees are away from their desks, all FTI must be secured. An example of a secured location is a locked filing cabinet or locked desk drawer.

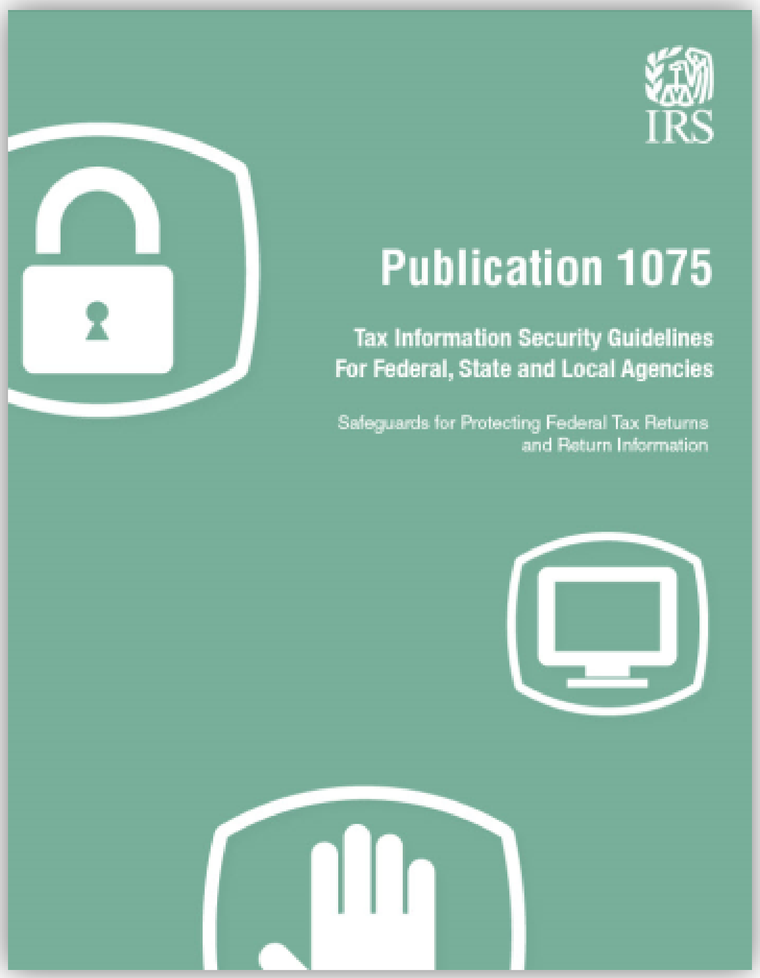
- Federal tax information sent to another location must be double-sealed (one envelope inside another envelope).

Internal Revenue Service

FTI Logs:

IRS requires that a tracking system is established to identify and track the location of electronic and non-electronic FTI where it is used from the time it is received to the date it is disposed of.

For examples of suggested tracking elements, see IRS Publication 1075: Section 3.2, pages 13 & 14.



IRS

Publication 1075

Tax Information Security Guidelines
For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns
and Return Information

IRS information, continued…

Important Reminder:

When IRS information is commingled with DTF files, either paper or electronic, the entire file is considered to be FTI and must be labeled and safeguarded in accordance with IRS requirements. The Inspection or Disclosure Limitation Labels used to identify all FTI are available from the Disclosure Unit located in Bldg. 8, Room 700.

Inspection or Disclosure Limitations
Unauthorized inspection or disclosure, printing, or publishing of any Federal return or return information, or any information therefrom, may be punishable by fine or imprisonment and in the case of Federal officers or employees, dismissal from office or employment. See section 7213 and 7213A of the Internal Revenue Code and 18 U.S.C. section 1905. In addition, code section 7431 provides for civil damages for unauthorized inspection or disclosure of such information. Tapes should be degaussed after they have served their purpose, disposed of in accordance with Publication 1075 disposition guidelines or returned to the IRS.
Department of the Treasury *Notice 129A (Rev.12-97)*
Internal Revenue Service *Cat No. 45547W*

<u>Definition:</u> *Commingling*: When Department information is combined with federal tax information, either paper or electronic, it is considered to be commingled and is to be treated as FTI.

Federal tax return and/or return information received directly from a taxpayer or third party is **NOT** considered FTI.

Electronic files must use a naming convention that clearly identifies the file as containing FTI for example: FED.filename or FTI.filename.

Social Security

Social Security Administration (SSA) Information:

DTF receives SSA data which is considered confidential federal information. The Death Match File is one of the files DTF receives from SSA.

Penalty provisions under U.S. Department of Commerce, National Technical Information Services (NTIS) Section 203 of the Bipartisan Budget Act of 2013, 15 CFR 1110.200 imposes a penalty of $1,000 for each of the below infractions:

- Unauthorized disclosure of the Death Match File Information.
- Use of any deceased individual's Death Match File information for any purpose other than a legitimate fraud prevention interest or a legitimate business pursuant to a law, governmental rule, regulation or fiduciary duty.

Law

Important Information:

You should be aware of several laws and legislative acts that address penalties if improper disclosure of confidential information occurs:

- ➢ Privacy Act of 1974
- ➢ New York State Tax Law
- ➢ New York State Penal Law
- ➢ Internal Revenue Code

Law

Privacy Act of 1974, 5 U.S.C. 552a:

Under Section 5 U.S.C 552a(i)(1) of the Privacy Act of 1974, it is unlawful for you to willfully disclose confidential information in any manner to any person not entitled to receive it. In doing so you would be guilty of a misdemeanor and fined up to $5,000.

Law

New York State Penalties:

Under New York State Tax Law Section 1825, it is a crime for you to make an unauthorized disclosure of confidential New York State Tax information.

New York State Penal Law Section 156 imposes additional charges for unauthorized access, computer trespass or computer tampering, which can be misdemeanors or felonies.

Punitive Actions For Violating NYS Tax Law:

- Possible dismissal from employment.
- Possible criminal prosecution.
- A fine up to $10,000, up to one year in jail, or both.
- Possible prohibition from holding state service for five years.

Law

Federal Penalties:

Under Section 7213 of the Internal Revenue Code, it is a felony to make an unauthorized disclosure of federal tax information.

Penalties Include:

- A fine up to $5,000, up to 5 years in prison, or both.
- Cost of prosecution.
- Possible disciplinary action.

Law

Federal Penalties, continued…

Under Section 7213A of the Internal Revenue Code, it is a crime to browse federal tax data without a business need.

<u>Penalties Include:</u>

- A fine not exceeding $1,000, imprisonment of not more than one year, or both.
- Cost of prosecution.

Law

Federal Penalties, continued…

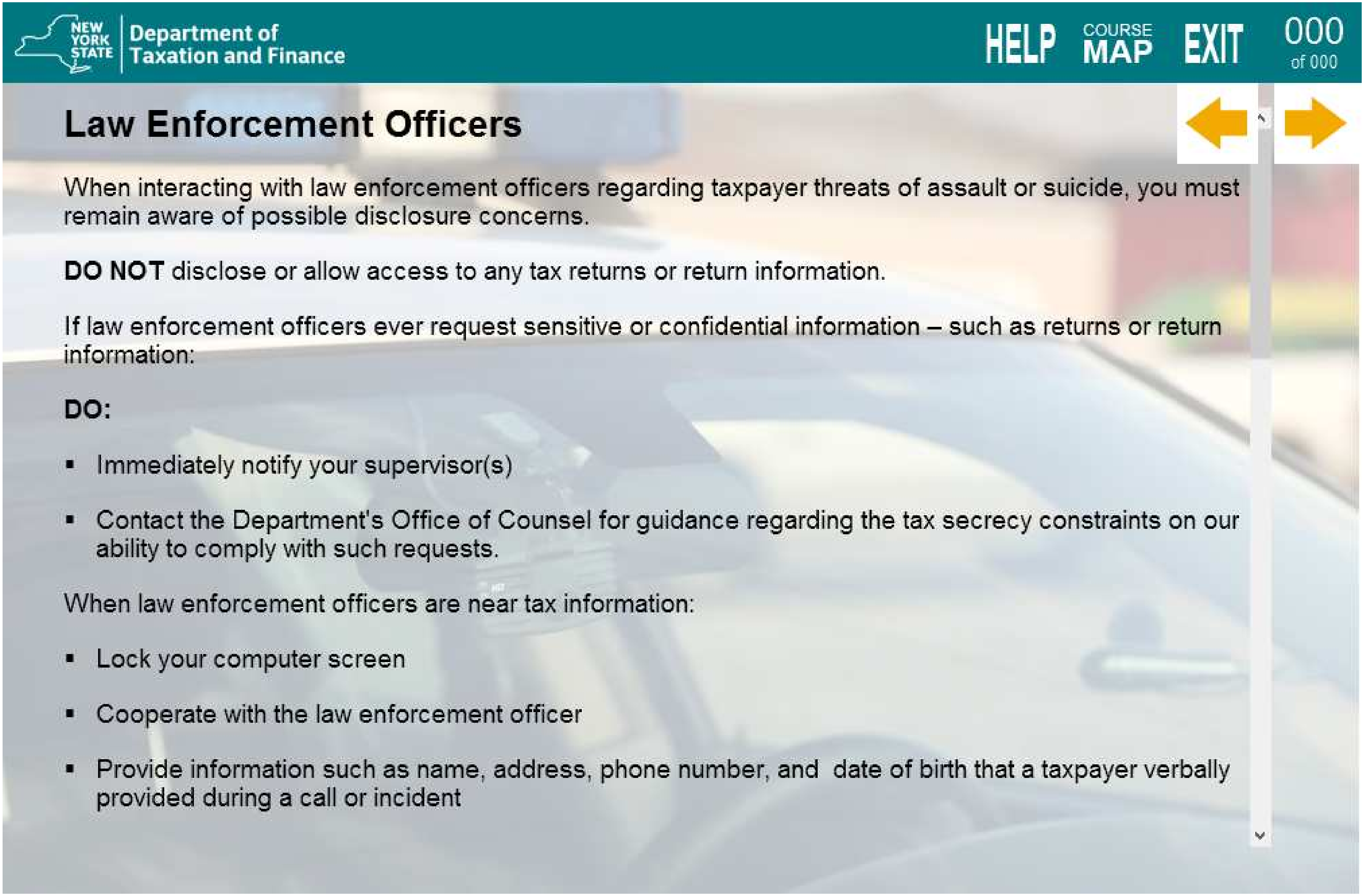
Federal Law, Section 7431, allows an affected taxpayer the right to file a civil lawsuit against you for browsing or for unauthorized disclosure (UNAX).

<u>Definition:</u>

UNAX: Willful, unauthorized inspection, access or browsing of federal tax information.

Law

Between 2014 and 2016, the Office of Internal Affairs investigated **20 individuals** who were criminally prosecuted for unlawful accessing, computer trespassing and tax secrecy violations. To date **18 have pled guilty**, including **six who pled to the violation** banning them from state service for five years. These cases generally involved employees or contractors looking up family members, friends, business associates and others' confidential tax information without a legitimate business reason to do so.



Law Enforcement Officers

When interacting with law enforcement officers regarding taxpayer threats of assault or suicide, you must remain aware of possible disclosure concerns.

DO NOT disclose or allow access to any tax returns or return information.

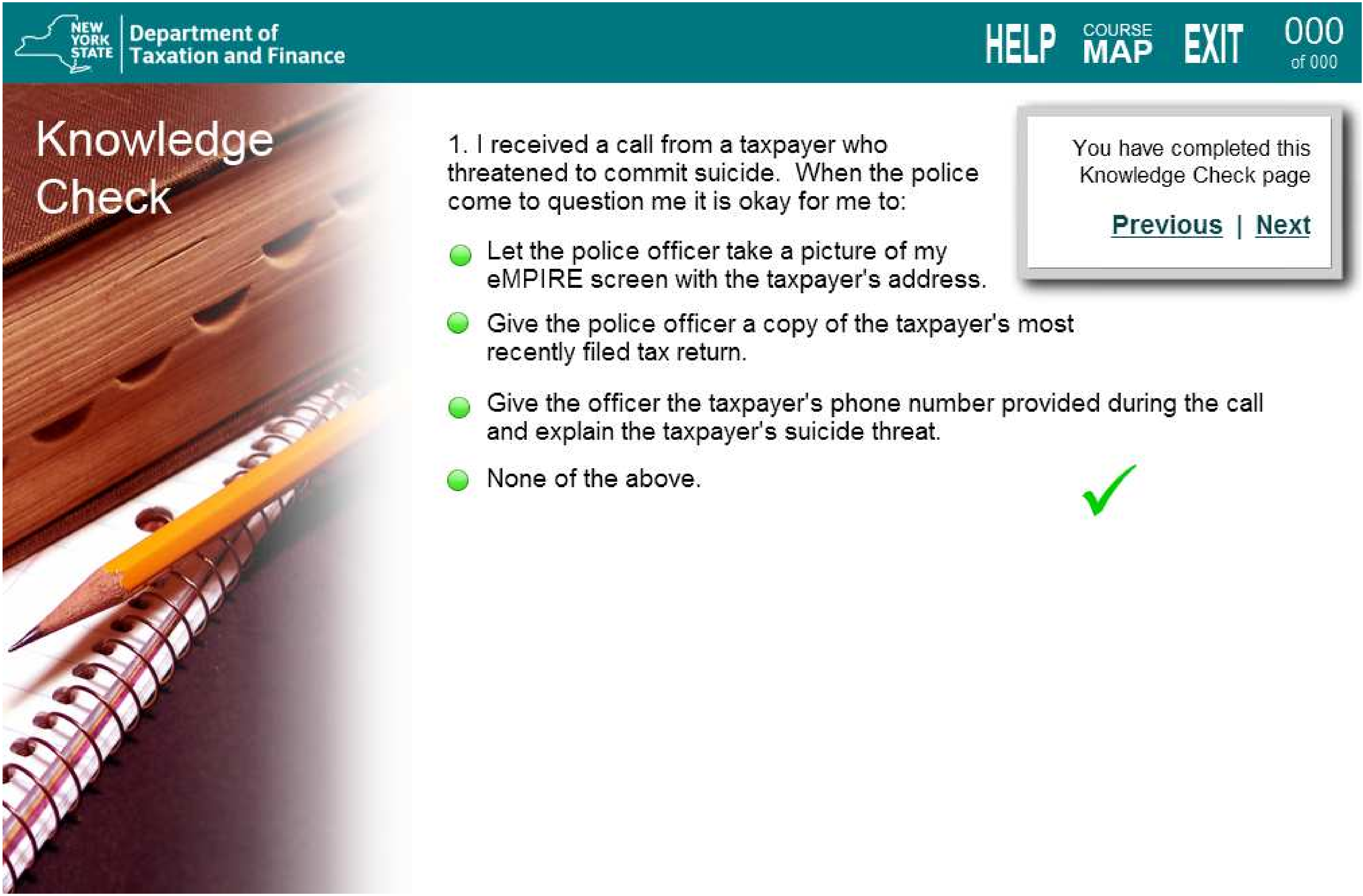
If law enforcement officers ever request sensitive or confidential information – such as returns or return information:

DO:

- Immediately notify your supervisor(s)
- Contact the Department's Office of Counsel for guidance regarding the tax secrecy constraints on our ability to comply with such requests.

When law enforcement officers are near tax information:

- Lock your computer screen
- Cooperate with the law enforcement officer
- Provide information such as name, address, phone number, and date of birth that a taxpayer verbally provided during a call or incident



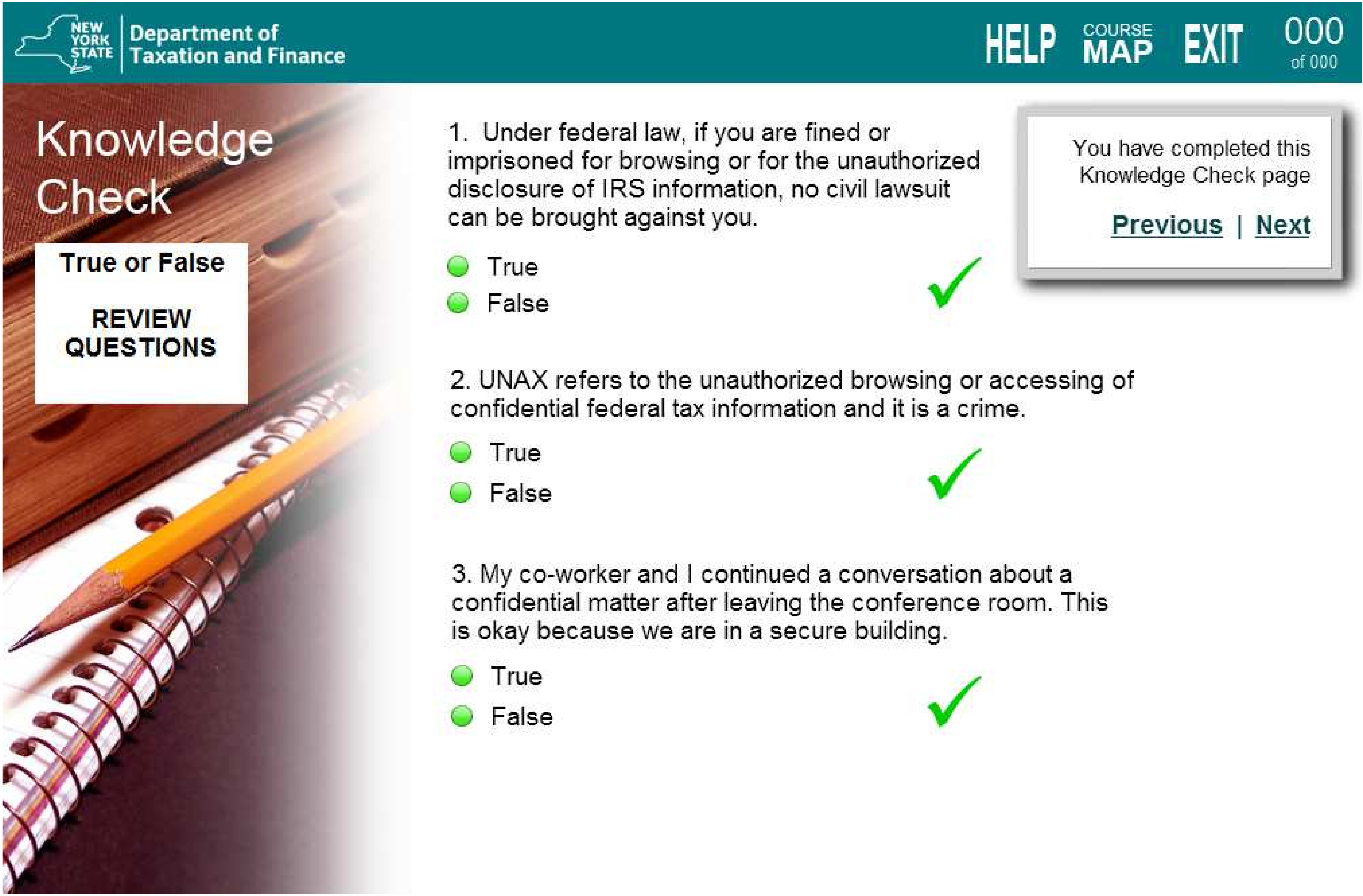
Knowledge Check

1. I received a call from a taxpayer who threatened to commit suicide. When the police come to question me it is okay for me to:

- ● Let the police officer take a picture of my eMPIRE screen with the taxpayer's address.
- ● Give the police officer a copy of the taxpayer's most recently filed tax return.
- ● Give the officer the taxpayer's phone number provided during the call and explain the taxpayer's suicide threat.
- ● None of the above. ✓

You have completed this Knowledge Check page

Previous | Next



Knowledge Check

True or False

REVIEW QUESTIONS

You have completed this Knowledge Check page

1. Under federal law, if you are fined or imprisoned for browsing or for the unauthorized disclosure of IRS information, no civil lawsuit can be brought against you.

● True

● False ✓

2. UNAX refers to the unauthorized browsing or accessing of confidential federal tax information and it is a crime.

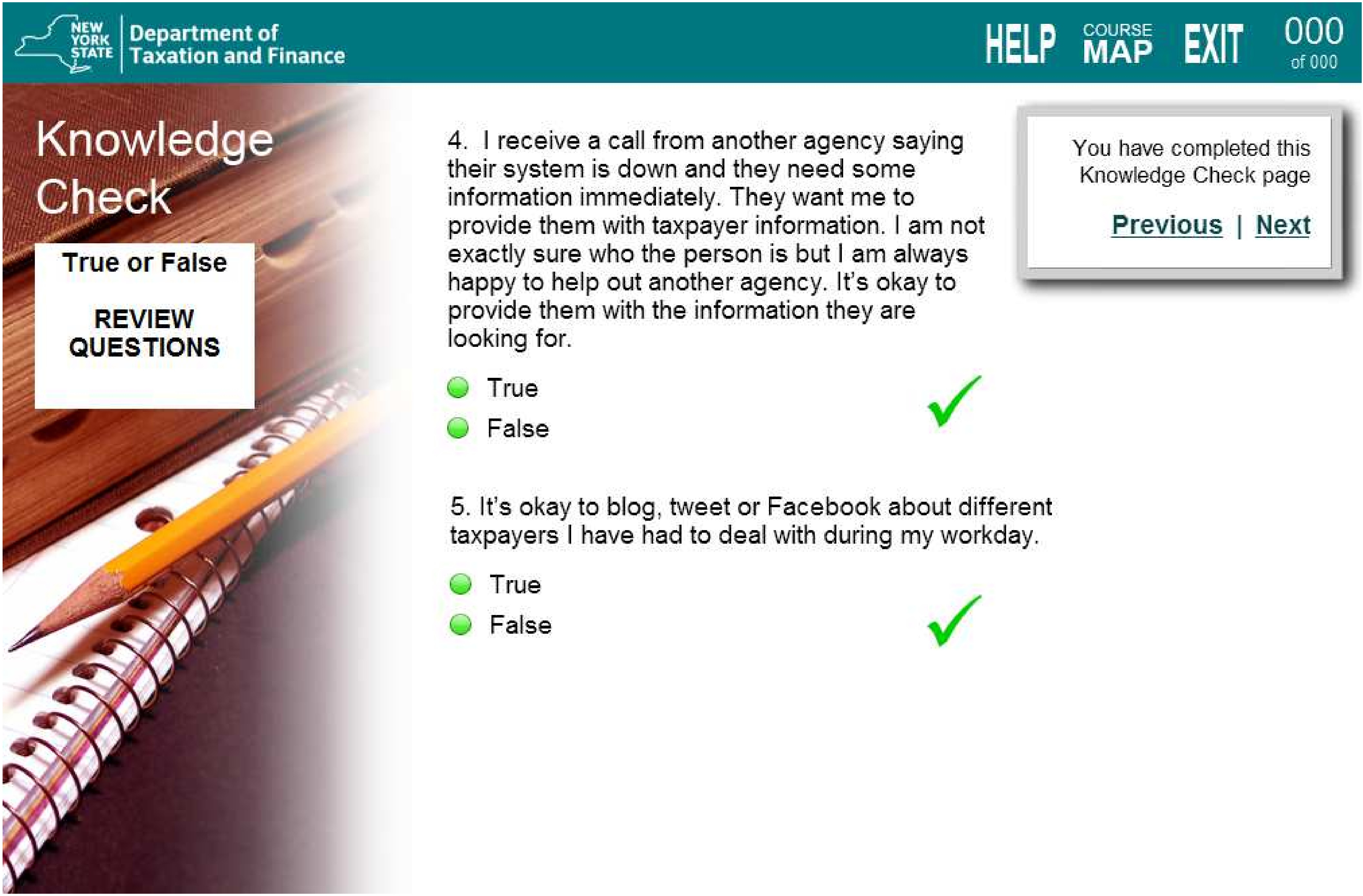
● True

● False ✓

3. My co-worker and I continued a conversation about a confidential matter after leaving the conference room. This is okay because we are in a secure building.

● True

● False ✓



Knowledge Check

True or False

REVIEW QUESTIONS

4. I receive a call from another agency saying their system is down and they need some information immediately. They want me to provide them with taxpayer information. I am not exactly sure who the person is but I am always happy to help out another agency. It's okay to provide them with the information they are looking for.

● True ✓

● False

5. It's okay to blog, tweet or Facebook about different taxpayers I have had to deal with during my workday.

● True

● False ✓

You have completed this Knowledge Check page

Frequently Asked Questions

Federal Tax Information Part 1:

Question: FTI obtained from e-MPIRE is written down on a separate piece of paper. Do I need to log this somewhere?

Answer: The information should be clearly labeled as Federal Tax Information and you need to keep a log of this information just like you would if you printed FTI.

Inadvertent Unauthorized Disclosure Part 1:

Question: What happens if, when accessing DTF computerized files, I make a typing error and end up pulling up a non-assigned case. Will I be accused of a UNAX violation?

Answer: No, accesses resulting from a typing error are **NOT** UNAX violations. A UNAX violation requires willful unauthorized access. Inadvertent or mistaken accesses are **NOT** violations of the law. This access should be noted in your access log with a note stating the circumstances.

Comments and Suggestions

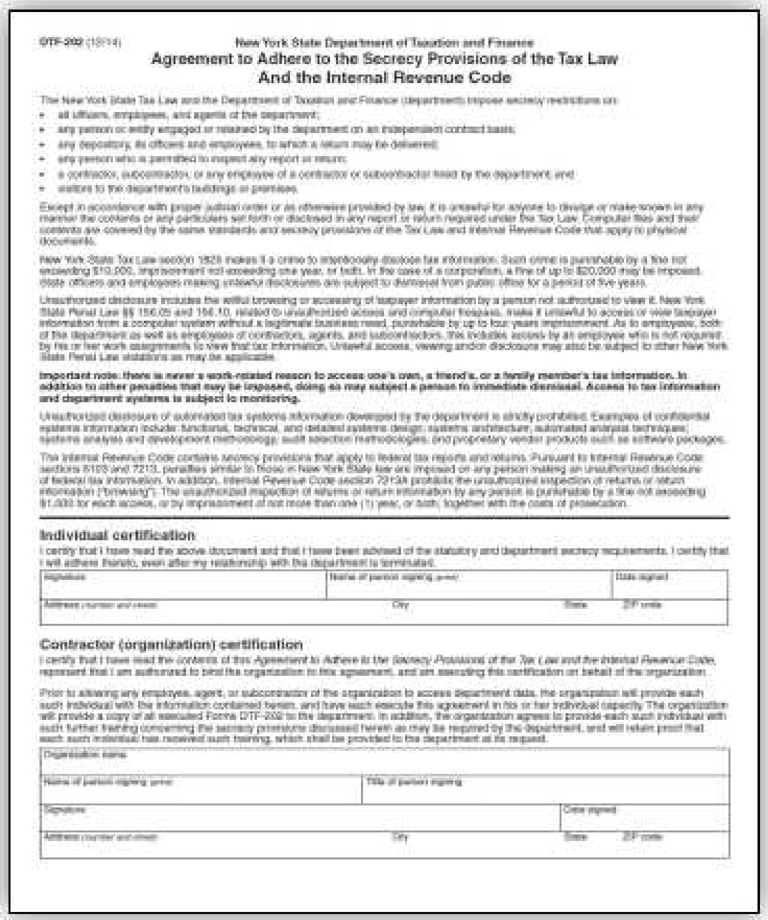
This training will be updated each year. If you would like a topic or have a question you would like addressed, please e-mail your comments or suggestions to the IRS Compliance Mailbox:

- [Tax.sm.orm.access.requests]

DTF- 202

- **DTF-202:** Agreement to Adhere to the Secrecy Provisions of the Tax Law and the Internal Revenue Code
- **Important:**

  Non- DTF Employees are required to read and agree to the secrecy provisions that are contained in the DTF-202.



DTF-202 (12/14)

New York State Department of Taxation and Finance

Agreement to Adhere to the Secrecy Provisions of the Tax Law And the Internal Revenue Code

The New York State Tax Law and the Department of Taxation and Finance (department) impose secrecy restrictions on:

- all officers, employees, and agents of the department;
- any person or entity engaged or retained by the department on an independent contract basis;
- any depository, its officers and employees, to which a return may be delivered;
- any person who is permitted to inspect any report or return;
- a contractor, subcontractor, or any employee of a contractor or subcontractor hired by the department; and
- visitors to the department's buildings or premises.

Except in accordance with proper judicial order or as otherwise provided by law, it is unlawful for anyone to divulge or make known in any manner the contents or any particulars set forth or disclosed in any report or return required under the Tax Law. Computer files and their contents are covered by the same standards and secrecy provisions of the Tax Law and Internal Revenue Code that apply to physical documents.

New York State Tax Law section 1825 makes it a crime to intentionally disclose tax information. Such crime is punishable by a fine not exceeding $10,000, imprisonment not exceeding one year, or both. In the case of a corporation, a fine of up to $20,000 may be imposed. State officers and employees making unlawful disclosures are subject to dismissal from public office for a period of five years.

Unauthorized disclosure includes the willful browsing or accessing of taxpayer information by a person not authorized to view it. New York State Penal Law §§ 156.05 and 156.10, related to unauthorized access and computer trespass, make it unlawful to access or view taxpayer information from a computer system without a legitimate business need, punishable by up to four years imprisonment. As to employees, both of the department as well as employees of contractors, agents, and subcontractors, this includes access by an employee who is not required by his or her work assignments to view that tax information. Unlawful access, viewing and/or disclosure may also be subject to other New York State Penal Law violations as may be applicable.

Important note: there is never a work-related reason to access one's own, a friend's, or a family member's tax information. In addition to other penalties that may be imposed, doing so may subject a person to immediate dismissal. Access to tax information and department systems is subject to monitoring.

Unauthorized disclosure of automated tax systems information developed by the department is strictly prohibited. Examples of confidential systems information include: functional, technical, and detailed systems design; systems architecture; automated analysis techniques; systems analysis and development methodology; audit selection methodologies; and proprietary vendor products such as software packages.

The Internal Revenue Code contains secrecy provisions that apply to federal tax reports and returns. Pursuant to Internal Revenue Code sections 6103 and 7213, penalties similar to those in New York State law are imposed on any person making an unauthorized disclosure of federal tax information. In addition, Internal Revenue Code section 7213A prohibits the unauthorized inspection of returns or return information ("browsing"). The unauthorized inspection of returns or return information by any person is punishable by a fine not exceeding $1,000 for each access, or by imprisonment of not more than one (1) year, or both, together with the costs of prosecution.

Individual certification

I certify that I have read the above document and that I have been advised of the statutory and department secrecy requirements. I certify that I will adhere thereto, even after my relationship with the department is terminated.

Signature	Name of person signing *(print)*		Date signed
Address *(number and street)*	City	State	ZIP code

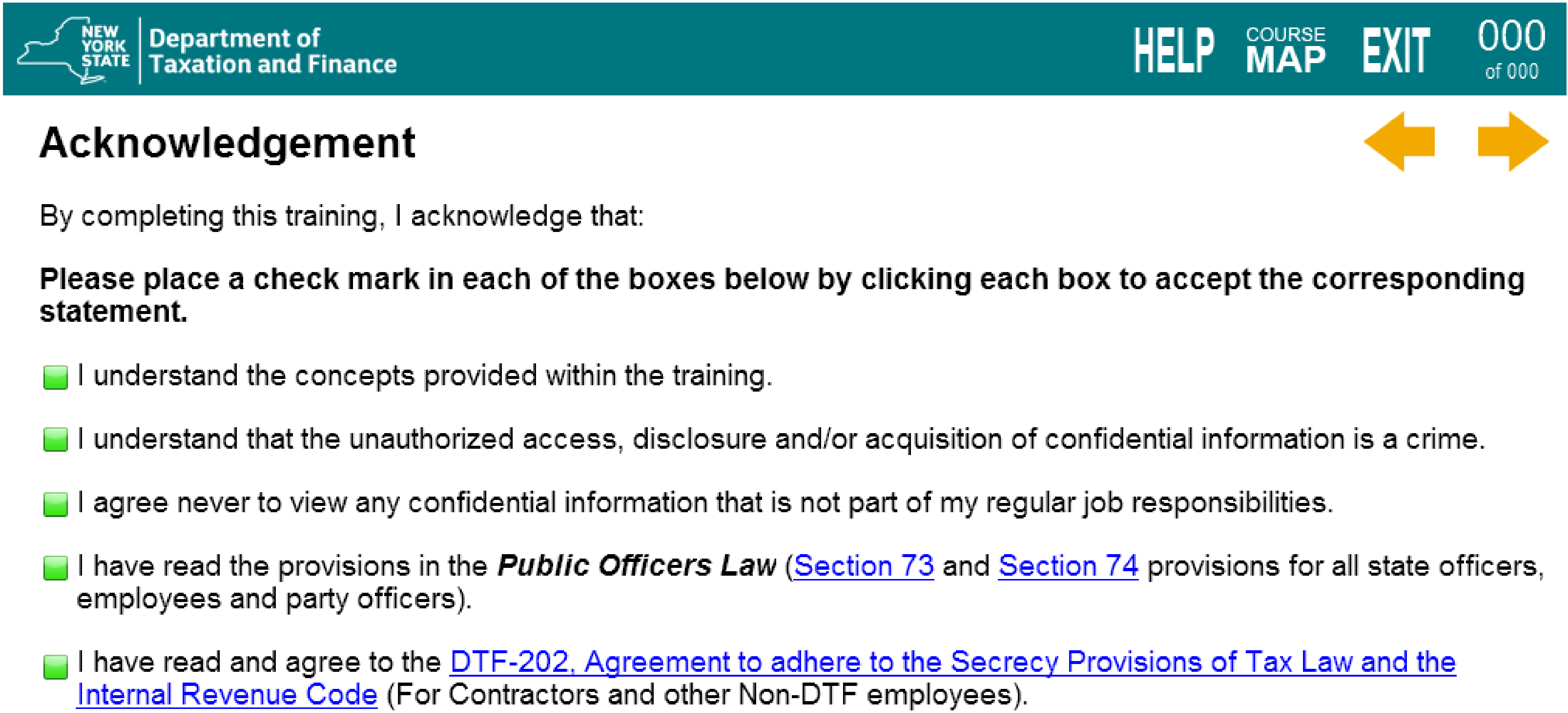
Contractor (organization) certification

I certify that I have read the contents of this *Agreement to Adhere to the Secrecy Provisions of the Tax Law and the Internal Revenue Code*, represent that I am authorized to bind the organization to this agreement, and am executing this certification on behalf of the organization.

Prior to allowing any employee, agent, or subcontractor of the organization to access department data, the organization will provide each such individual with the information contained herein, and have each execute this agreement in his or her individual capacity. The organization will provide a copy of all executed Forms DTF-202 to the department. In addition, the organization agrees to provide each such individual with such further training concerning the secrecy provisions discussed herein as may be required by the department, and will retain proof that each such individual has received such training, which shall be provided to the department at its request.

Organization name			
Name of person signing *(print)*	Title of person signing		
Signature			Date signed
Address *(number and street)*	City	State	ZIP code

Click to view



Acknowledgement

By completing this training, I acknowledge that:

Please place a check mark in each of the boxes below by clicking each box to accept the corresponding statement.

🟩 I understand the concepts provided within the training.

🟩 I understand that the unauthorized access, disclosure and/or acquisition of confidential information is a crime.

🟩 I agree never to view any confidential information that is not part of my regular job responsibilities.

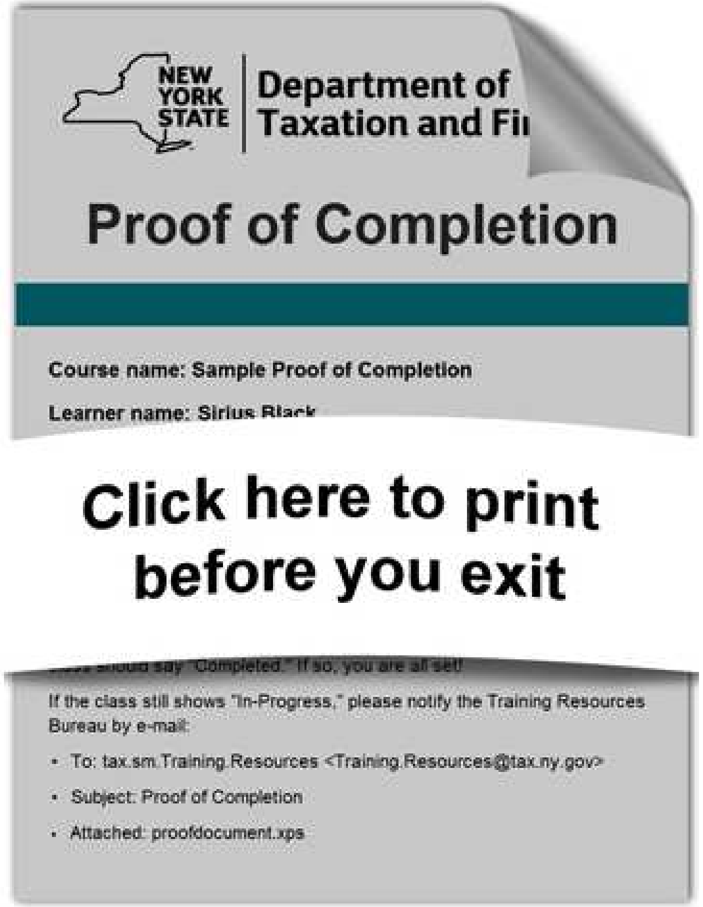
🟩 I have read the provisions in the ***Public Officers Law*** (Section 73 and Section 74 provisions for all state officers, employees and party officers).

🟩 I have read and agree to the DTF-202, Agreement to adhere to the Secrecy Provisions of Tax Law and the Internal Revenue Code (For Contractors and other Non-DTF employees).

That's it!

You have completed the training. Click on the image to the right to view and save your *Proof of Completion*, which you will need if anything goes wrong saving this session.

Use the exit button when you are done so that your progress is saved.



NEW YORK STATE | Department of Taxation and Fi

Proof of Completion

Course name: Sample Proof of Completion

Learner name: Sirius Black

Click here to print before you exit

should say "Completed." If so, you are all set!

If the class still shows "In-Progress," please notify the Training Resources Bureau by e-mail:

- To: tax.sm.Training.Resources <Training.Resources@tax.ny.gov>
- Subject: Proof of Completion
- Attached: proofdocument.xps

NEW YORK STATE | Department of Taxation and Finance

Proof of Completion

Course name:

Learner name:

Learner ID:

Completion date:

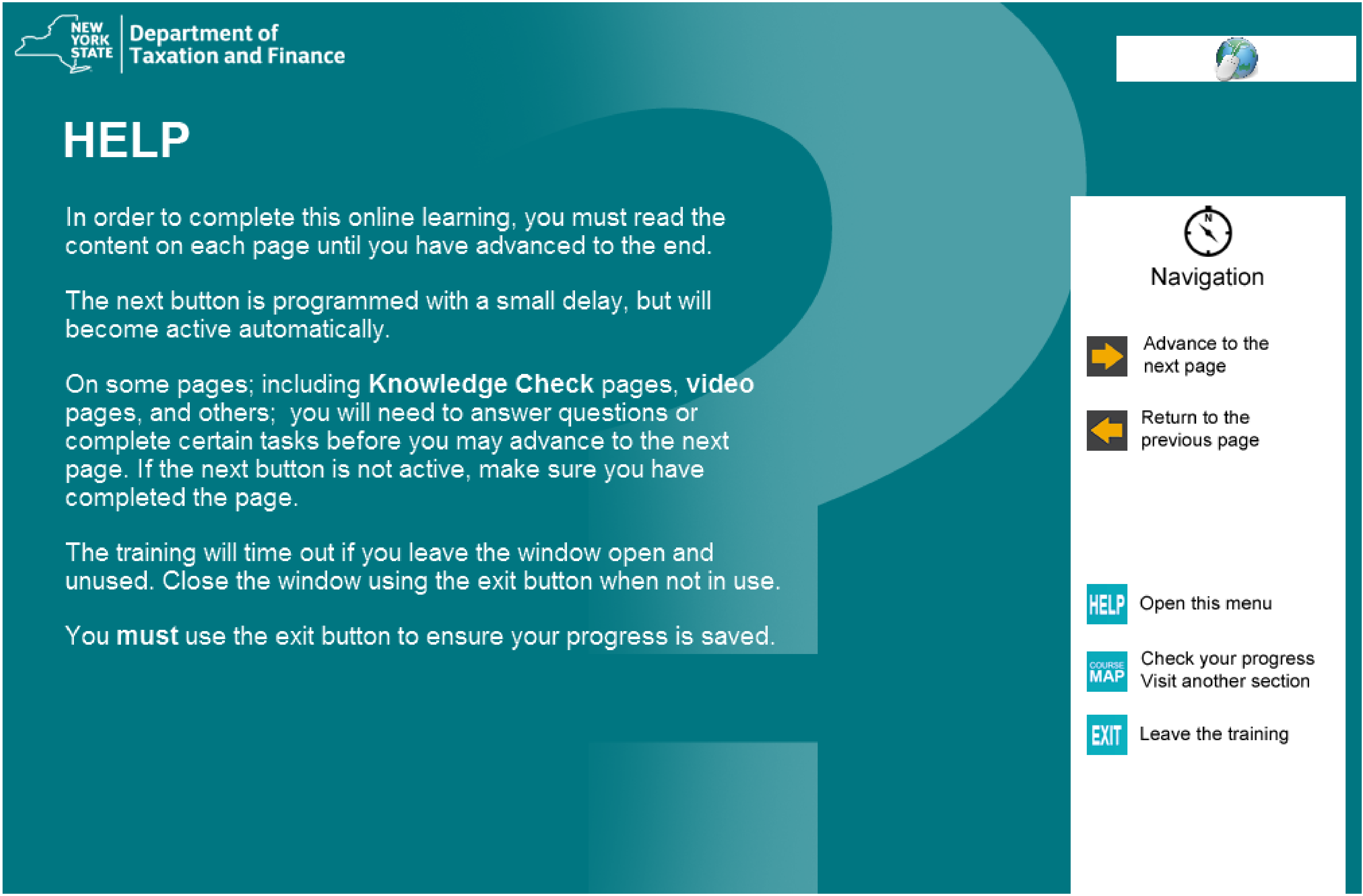
Instructions

Please print (ctrl-p) this document. To make it a digital copy, you can choose "Microsoft XPS Document Writer" as your printer.

After you exit this class, return to your My Learning page. The status of this class should say "Completed." If so, you are all set!

If the class still shows "In-Progress," please notify the Training Resources Bureau by e-mail:

- To: tax.sm.Training.Resources <Training.Resources@tax.ny.gov>
- Subject: Proof of Completion
- Attached: proofdocument.xps



NEW YORK STATE | Department of Taxation and Finance

HELP

In order to complete this online learning, you must read the content on each page until you have advanced to the end.

The next button is programmed with a small delay, but will become active automatically.

On some pages; including **Knowledge Check** pages, **video** pages, and others; you will need to answer questions or complete certain tasks before you may advance to the next page. If the next button is not active, make sure you have completed the page.

The training will time out if you leave the window open and unused. Close the window using the exit button when not in use.

You **must** use the exit button to ensure your progress is saved.

Navigation

➡	Advance to the next page
⬅	Return to the previous page
HELP	Open this menu
COURSE MAP	Check your progress Visit another section
EXIT	Leave the training

NEW YORK STATE | Department of Taxation and Finance

COURSE MAP

YOU ARE HERE

gress Bar