



TD AMERITRADE releases the results of its client SPAM investigation.

What you should know:

- While investigating client reports of SPAM, we recently discovered and eliminated unauthorized code that allowed an external source to retrieve certain client information from one of our databases.
- At no time were clients' financial assets held at TD AMERITRADE touched as a result of this issue. UserIDs and passwords were not stored in this particular database.
- Although sensitive information, like Social Security Numbers, is stored in this database, we've concluded that this information belonging to our legacy TD Waterhouse clients was not taken.
- We also have no evidence that this information belonging to our legacy Ameritrade clients was taken and have further validated with a third-party expert that there is no evidence that any of our clients have been subject to identity theft as a result of this issue.
- We are confident that we have eliminated the unauthorized code and have taken the actions necessary to prevent it from recurring.
- This issue is larger than TD AMERITRADE and is something that all companies involved in e-commerce should be aware of and prepared to address. We participate in industry peer groups to share information on these types of threats in the interest of protecting all of our clients.

We understand that the increase in unwanted SPAM caused by this issue is annoying and an inconvenience to clients. We sincerely apologize for that and any added concern this may have caused.

For additional information, please see the FAQs provided below.

Frequently Asked Questions (FAQs)

Q. What happened?

Through an ongoing investigation of stock-related SPAM, we recently discovered and eliminated unauthorized code from our systems that allowed a third party to retrieve certain client information stored in one of our databases.

We found the code, eliminated it and put in steps to prevent it from recurring.

While this issue may have created an increase in SPAM for our clients, you should know that **the assets in our clients' accounts held with us remain secure**. Account UserIDs and passwords, which are necessary to access an account, were not stored in this particular database.

Q. What are you doing about it?

We eliminated the unauthorized code identified in our systems and made changes to prevent this issue from recurring.

We contacted the proper authorities and are working with them to track down responsible parties. We are communicating with our clients and are addressing their questions as they are raised.

We have also hired a third party, ID Analytics, which specializes in identity risk, to monitor potential identity theft. After a thorough initial evaluation, the firm found no evidence of identity theft as a result of this issue. We are retaining its services on an ongoing basis to continue to monitor for evidence of identity theft.

Q. Who is ID Analytics, and what specifically will they do for TD AMERITRADE?

ID Analytics, Inc. is a San Diego-based company that specializes in identity risk. Many of the country's largest banks, wireless carriers, healthcare providers, retailers, mortgage companies and government entities rely on its services to prevent identity fraud.

You should know that ID Analytics has passed an extensive on-site security audit, which we require of all our vendors and especially those that we entrust with our clients' information. ID Analytics is monitoring potential identity theft for us as a result of this issue.

For more specific information on its processes, please visit www.idanalytics.com.

Q. What information was taken from the database, and who is affected?

This particular database included information on clients, accounts, demographics and trading activity.

We do know that information such as email addresses, names, addresses, phone numbers, and other miscellaneous account information, such as number of trades placed in a given time period was retrieved from this database and that this activity affected TD AMERITRADE retail and institutional clients who were clients prior to July 18.

While more sensitive information like account numbers, date of birth and Social Security Numbers was also stored in this particular database, we have no evidence that it was retrieved or used to commit identity theft. **In fact, we have been able to conclude that this sensitive information belonging to our legacy TD Waterhouse retail and institutional clients was not retrieved.**

Q. How do you know that this sensitive information, like Social Security Numbers, hasn't been leaked or misused?

After extensive investigations involving outside forensics experts, we have no evidence that this sensitive personal information was taken.

That is one of the reasons why we have also hired ID Analytics. Its initial investigation has concluded that there is no evidence of identity theft as a result of this issue.

Because of our ongoing investigation, we will not provide additional details.

Q. If information such as email addresses has been compromised for the legacy TD Waterhouse clients, how can you be certain that more sensitive information was not?

Information on our legacy TD Waterhouse clients has been stored in this database for a shorter time. Because of this, we have been able to conclude that this sensitive information was not retrieved.

Q. Does this issue affect new accounts as well? At what point are clients not affected?

Through our investigation we have been able to establish that any new client who opened an account at TD AMERITRADE after July 18, 2007, is not affected.

Q. How long has this issue been going on?

Unfortunately, the issue of SPAM is an industry issue that has been increasing over the past few years. There are many different SPAM campaigns that affect almost every person with an email



address. We were investigating a stream of stock-related SPAM sent to our clients when we discovered this particular issue. The investigation had been going on for some time.

Because of our ongoing investigation, we cannot provide further details. One of the most important things is that we have eliminated the unauthorized code and taken action to prevent it from recurring.

Q. Don't you have systems in place to prevent intrusions such as these?

Yes. However, for the security of these systems, and so as to not compromise the ongoing investigation, we will not provide further details about the intrusion.

Q. Have you discovered the perpetrator(s)? When will you have more information?

We are working with the appropriate authorities to track down the perpetrators and to gather as much information as possible as quickly as possible for the benefit of our clients.

Q. Have any of your peers been affected by this same issue?

We do not know at this point, as we are focused on the issue internally to protect our clients and their assets. However, we do know that SPAM is an industry concern.

We also know that criminals are increasingly using the Internet to commit fraudulent activities.

We believe this a problem that is broader than just our peers and that all companies should be aware of and prepared to address it. We participate in an industry peer group to discuss these matters in the interest of protecting all of our clients.

Q. What can clients do? How can they tell whether or not their information is secure?

Clients do not need to do anything with their accounts, other than remain alert in guarding their personal information.

Clients can change their account password(s) – it's not necessary, but clients are welcome to do so and should do so regularly as a matter of best practices

Clients can contact one of the three credit bureaus and request a copy of their credit report.

- Equifax: www.equifax.com
- Experian: www.experian.com
- TransUnion: www.tuc.com

For more information, clients can visit the [TD AMERITRADE online Security Center](#), for more tips and helpful information that relates to information security.

Q. Are clients at risk for identity theft?

We believe it is unlikely that identity theft will occur as a result of this issue.

While more sensitive information such as account numbers, date of birth and Social Security Numbers was stored in this database, we have no evidence to establish that it was retrieved or used to commit identity theft. In fact, we have been able to conclude that this sensitive information belonging to our legacy TD Waterhouse retail and institutional clients was not retrieved.



Remember, we have hired ID Analytics to monitor for potential identity theft. We are retaining their services on an ongoing basis to further help support our clients' accounts by continually monitoring for evidence of identity theft.

We also remind our clients that if some unauthorized activity were to take place in TD AMERITRADE accounts, clients are protected through our [Asset Protection Guarantee](#).

Q. Has this happened before to TD AMERITRADE?

No. We have made changes to our systems to prevent it from recurring.