WISCONSIN STATE PUBLIC DEFENDERS
Mission driven. Client centered.

Frequently Asked Questions about Release of Confidential Client Information

October 20, 2025

What happened?

The SPD inadvertently released confidential information to an individual while fulfilling an open records request. Below are some common questions people have about what was released, the steps we have taken, and the steps affected individuals can take.

What information was involved in this incident?

Numerous client names, addresses, and social security numbers were inadvertently released. In other cases, a client list which included client names, case county information, case numbers, and dates of birth was released. The client list did not involve case information or the clients' case files.

How does someone know if they are affected by this inadvertent release of confidential information?

We have contacted the affected parties by mail. If you did not receive a letter and you want to find out if your information was released during the inadvertent disclosures, please contact the SPD hotline at 800-445-2230 or spdhotline@opd.wi.gov.

What steps has the SPD taken since this incident?

The person who received the information immediately contacted us and notified law enforcement. We instructed the person who received the inadvertent disclosure to destroy the information and we have received confirmation that it has been destroyed. The report

containing this confidential information has also been discontinued. At this time, there is no indication that the information has been misused.

We have offered affected individuals an opportunity to enroll in free credit monitoring and identity theft protection service. We are offering this service for 12 months through IdentifyIQ. The plan includes:

- Bureau Credit Monitoring: Actively monitors credit for indicators of fraud from one credit bureau.
- Dark Web Monitoring: Technology searches the web, chat rooms, and bulletin boards 24/7 to identify trading or selling of personal information on the dark web.
- Identity Restoration: Identity restoration specialists are available to help address credit and non-credit related fraud.
- Up to $25,000 Identity Theft Insurance: Provides coverage for certain costs and unauthorized electronic fund transfers. An Identity Restoration team will guide affected parties through the recovery process. *This description is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Any affected party will need to refer to the actual policies for terms, conditions, and exclusions of coverage after enrollment.*
- The deadline to enroll in the credit monitoring program is February 3, 2026.

What if people have questions about the IdentityIQ service?

If people called into our hotline requesting credit monitoring and identity theft protection and still have questions about the IdentityIQ service, they should contact IDIQ's customer service team at 1-877-875-IDIQ (4347), Monday - Friday 7:00 am to 6:00 pm CT and Saturdays 8:30 am to 5:00 pm CT. The affected party will have to provide their activation code in order for IdentityIQ to answer questions about services.

What if people don't want to use the credit monitoring service offered?

People who do not want to use the credit monitoring service offered by the SPD are not under any obligation to use it.

What other ways can personal information be protected?

The Federal Trade Commission (FTC) recommends people place a free fraud alert on their credit file. This tells creditors to contact the person before opening new accounts or changing existing ones. People can contact any of the three major credit bureaus to do this.

How does a person place a fraud alert on their credit file?

People can contact Equifax at equifax.com/personal/credit-report-services or 1-800-685-1111; Experian at experian.com/help or 1-888-397-3742; or TransUnion at transunion.com/credit-help or 1-888-909-8872. Once one bureau confirms the fraud alert, the others will be notified. It stays on a person's report for one year and can be renewed.

Should people check their credit report?

Yes, people should ask each credit bureau to send them a free credit report after placing a fraud alert. People should review the reports for any unrecognized accounts or inquiries, which could be signs of identity theft. The FTC also recommends periodic checks of credit reports.

What should someone do if they find suspicious activity or that their information has been misused?

If someone's personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps.

What is a credit freeze and how does someone place one?

A credit freeze prevents potential creditors from accessing a person's credit report, making it less likely for an identity thief to open new accounts in a person's name. People can place a freeze by contacting **each** of the major credit bureaus (address and email above) for fraud alerts. A freeze remains in place until the person asks the credit bureau to lift or remove it.

If a person requests a credit freeze online or by phone, then the credit reporting agencies have one business day after receiving the request to place a credit freeze on their credit file report. If the person requests a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one hour. If a person requests a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three business days after getting the request.

People **must** separately place a credit freeze on their credit file at **each** credit reporting agency. The following information should be included when requesting a credit freeze:

- Full name, with middle initial and any suffixes
- Social Security number
- Date of birth (month, day, and year)
- Current address and previous addresses for the past five (5) years
- Proof of current address, such as a current utility bill or telephone bill
- Other personal information as required by the applicable credit reporting agency

Where can a person find more information about protecting themselves from identity theft?

The FTC's website, IdentityTheft.gov/databreach, has information about steps people can take to help protect themselves, based on the types of information exposed in this breach.

Who can people contact if they have more questions?

They can contact us at 1-800-445-2230 or SPDhotline@opd.wi.gov. They can also seek assistance or file a complaint through Wisconsin's Department of Agriculture, Trade and Consumer Protection (DATCP) at DATCPHotline@wi.gov or 800-422-7128.

They may also contact the FTC at **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338), to learn more about identity theft and the steps they can take to protect yourself and prevent such activity.

Does this release affect pending cases?

No. The inadvertent disclosure does not affect any pending cases. The disclosure did not include any information regarding the client's charges, discovery, or any confidential case information the client provided to our staff.

Does the SPD have power to change the resolution of pending case(s) because of this inadvertent disclosure?

No. SPD has no power or authority to affect the resolution of any pending case due to the inadvertent disclosure. This disclosure does not affect the outcome of your case. Confidential case information was not disclosed.

Can people affected make a police report or contact another agency or person?

Yes. Clients may report the inadvertent disclosure to anyone or any agency. SPD has followed the guidance from the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) and the Wisconsin Department of Justice; SPD has fulfilled its obligations under the law.

Has the SPD taken any steps to increase the protection of SSNs?

Yes. We have changed the collection and storage of SSN information to increase the protection of personally identifiable information.

Does the SPD provide a method for removing client SSNs?

Yes. If requested by a client, and the case(s) has been completed, a client can request to have their SSN removed from their electronic case file. If the former client applies for a public defender in the future, they will be asked for the last 4 digits of their SSN to determine eligibility as required by Wis. Stat. 977.06.