

R011151-100324 - Open Records Request

Message History (17)

✉ On 2/26/2025 5:58:02 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

February 26, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

A Varonis risk assessment helped this org get their data under control

<https://www.youtube.com/watch?v=2Gi9Iwcil7g>

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you

must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: Thank you for your continued patience. Unfortunately, the logs you have requested are no longer available. The IT Department's retention policy regarding this type of information is only for 31 days.

For additional information regarding the Local Government Record Retention Schedules, click [here](#).

For additional information regarding the Fulton County Municode as it relates to records management, click [here](#).

Below are the traffic views for fultoncountyga.gov/districtattorney:

December 2023 – 5,247

January 2024 – 16,194

February - 39,223

March 2024 – 27,125

April 2024 – 9,212

May 2024 – 11,925
June 2024 - 9,469
July 2024 – 5,723
August 2024 – 7,233
September 2024 – 10,182

Sincerely,

Open Records Team

✉ On 2/18/2025 9:30:00 AM, orr@fultoncountygga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



OPEN RECORDS
TELEPHONE (404) 612-0281

February 18, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

A Varonis risk assessment helped this org get their data under control

<https://www.youtube.com/watch?v=2Gi9Iwcil7g>

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We are working along with the IT Department to determine if there are any responsive documents. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Friday, February 28, 2025. We appreciate your continued patience.

Sincerely,

Open Records Team

✉ On 2/7/2025 1:49:00 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**OPEN RECORDS
TELEPHONE (404) 612-0281**

February 07, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you

must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
 - *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
 - *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
 - *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
 - *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
 - *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
 - *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, additional time is needed to fulfill your open records request. We have requested another update from the IT Department regarding your the status of your request. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Tuesday, February 18, 2025. We appreciate your continued patience.

Sincerely,

Open Records Team

✉ On 1/27/2025 11:24:05 AM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

January 27, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountytga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

• *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.)*

were accessed, who accessed them (IP addresses), and the time of access.

- *Error Logs:* These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.
 - *Audit Logs:* These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.
 - *Transaction Logs:* This is a sequential record of all database transactions, showing what data was modified or deleted
 - *Security Logs:* Track user authentication, permissions changes, and potential security incidents that might relate to deletions
 - *Event Logs:* Windows or Linux event logs can track file system and user activity that might indicate deletions
 - *Version Control Logs (if applicable)* If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, additional time is needed to fulfill your open records request. Your request is still in line to be processed by the IT Department. We anticipate an update or response will be forwarded to you within 5 business days or no later than 5:00 p.m. on Monday, February 3, 2025. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
County Attorney's Office

✉ On 1/16/2025 1:41:02 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

January 16, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountytga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

• *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.)*

were accessed, who accessed them (IP addresses), and the time of access.

- *Error Logs:* These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.
 - *Audit Logs:* These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.
 - *Transaction Logs:* This is a sequential record of all database transactions, showing what data was modified or deleted
 - *Security Logs:* Track user authentication, permissions changes, and potential security incidents that might relate to deletions
 - *Event Logs:* Windows or Linux event logs can track file system and user activity that might indicate deletions
 - *Version Control Logs (if applicable)* If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, additional time is needed to fulfill your open records request. Your request is still in line to be processed by the IT Department. We anticipate an update or response will be forwarded to you within 5 business days or no later than 5:00 p.m. on Friday, January 24, 2025. We appreciate your continued patience.
Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 1/6/2025 10:47:02 AM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324
Body:



FULTON COUNTY

OPEN RECORDS
TELEPHONE (404) 612-0281

January 06, 2025

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountytga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

• *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.)*

were accessed, who accessed them (IP addresses), and the time of access.

- *Error Logs:* These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.
- *Audit Logs:* These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.
- *Transaction Logs:* This is a sequential record of all database transactions, showing what data was modified or deleted
- *Security Logs:* Track user authentication, permissions changes, and potential security incidents that might relate to deletions
- *Event Logs:* Windows or Linux event logs can track file system and user activity that might indicate deletions
- *Version Control Logs (if applicable)* If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. Your request is still in line to be processed by the IT Department. We anticipate we will receive an update or response from them within 7 business days or no later than 5:00 p.m. on Wednesday, January 15, 2025. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 12/16/2024 11:12:04 AM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

December 16, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountytga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

• *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.)*

were accessed, who accessed them (IP addresses), and the time of access.

- *Error Logs:* These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.
 - *Audit Logs:* These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.
 - *Transaction Logs:* This is a sequential record of all database transactions, showing what data was modified or deleted
 - *Security Logs:* Track user authentication, permissions changes, and potential security incidents that might relate to deletions
 - *Event Logs:* Windows or Linux event logs can track file system and user activity that might indicate deletions
 - *Version Control Logs (if applicable)* If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, additional time is needed to fulfill your open records request. Your request is still in line to be processed by the IT Department. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Thursday, January 2, 2025. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 11/26/2024 11:29:01 AM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



FULTON COUNTY

OPEN RECORDS
TELEPHONE (404) 612-0281

November 26, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Monday, December 9, 2024. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 11/12/2024 5:55:02 PM, orr@fultoncountygga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

November 12, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Thursday, November 21, 2024. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 11/3/2024 12:21:02 AM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



OPEN RECORDS
TELEPHONE (404) 612-0281

November 03, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We anticipate an update or response will be forwarded to you within 5 business days or no later than 5:00 p.m. on Friday, November 8, 2024. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

✉ On 10/25/2024 9:54:02 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

October 25, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We anticipate an update or response will be forwarded to you within 5 business days or no later than 5:00 p.m. on Friday, November 1, 2024. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
Office of the County Attorney

← On 10/23/2024 10:00:26 AM, Billy Blume wrote:

TO: "Fulton County Georgia"[fultoncountyga@mycusthelp.net]

You lost the lawsuit in the Merchant case. So far Terrence has denied the records by making me go through the portal. The email was sent to him directly and he may be sued in his individual capacity and his official capacity. I highly advise you process my request before I pursue litigation. Server logs are easy, here are detailed instructions on how to obtain each:

To obtain the logs you're seeking, here's a guide for each type: 1. Access Logs

These logs are typically maintained by the web server (e.g., Apache, Nginx). Here's how to request them:
For Websites Hosted by a Third Party: Contact your hosting provider and submit a formal request for the access logs of your website. Specify the time period and details you need. Keywords: Access logs, server logs, IP addresses, request logs, time of access. Open Records Request: If the website is related to a government entity, you can file an open records request for these logs under state public records laws. Make sure to specify the type of server, the relevant time period, and any specific IP addresses of interest.
For Self-Hosted Websites: You can directly access the logs via your server's file system. Instructions (e.g., Linux): `cd /var/log/apache2/` (for Apache) or `cd /var/log/nginx/` (for Nginx), then use a command like `cat access.log`.

2. Error Logs
Error logs document any issues that occur with server operations.

For Websites Hosted by a Third Party: Request the error logs from your hosting provider. Specify the nature of errors you're looking for (e.g., file deletion issues) and the time frame. Keywords: Server error logs, HTTP error logs, failed access attempts, file deletion errors. Open Records Request: If dealing with a government entity's website, mention the nature of the errors (server issues, deletion failures) when making the request.

For Self-Hosted Websites: You can locate error logs on your server. Instructions (e.g., Linux): For Apache: `cd /var/log/apache2/`, then `cat error.log`. For Nginx: `cd /var/log/nginx/` then `cat error.log`.

3. Audit Logs
Audit logs track changes made to a database, including who made the changes.

For Websites Hosted by a Third Party: Request audit logs directly from your hosting provider. Clarify that you're looking for changes made to the database, particularly any deletions or alterations of records. Keywords: Audit logs, database changes, deleted entries, altered records. Open Records Request: For government-related websites, ask for any database audit logs, specifying the type of changes or deletions you're investigating.

For Self-Hosted Databases: If using MySQL, you can enable audit logging or check existing logs with the following: Instructions: `SHOW TABLES FROM mysql;` then `SELECT * FROM audit_log;` (if auditing is enabled).

4. Transaction Logs
Transaction logs show a sequential record of all database transactions.

For Websites Hosted by a Third Party: Contact your hosting provider and request access to the transaction logs, especially if you're investigating deleted or modified data. Keywords: Database transaction logs, deleted data, modified data, sequential records. Open Records Request: If applicable, request the database's transaction logs from a government entity's hosting provider. Provide a clear description of the specific transactions you're investigating.

For Self-Hosted Databases: For MySQL, transaction logs can be found by accessing the binary logs: Instructions: Enable binary logging in MySQL, then use `mysqlbinlog` to read the logs: `mysqlbinlog /var/log/mysql/mysql-bin.000001`.

5. Security Logs
Security logs track user authentication and permissions changes.

For Websites Hosted by a Third Party: Submit a request for security logs that document user authentication, permission changes, or potential security incidents. Specify the time period and any suspicious behavior you're investigating. Keywords: Security logs, user authentication, permission changes, security incidents. Open Records Request: For government websites, specify that you want to review logs concerning authentication and permission changes. Be clear about the dates or user accounts involved.

For Self-Hosted Websites: Check your server's security logs. Instructions (e.g., Linux): For Linux systems, security logs are typically found in `/var/log/auth.log` or `/var/log/secure`.

6. Event Logs
Event logs track system and user activity, often giving insights into file deletions.

For Websites Hosted by a Third Party: Ask your hosting provider for access to system or event logs that may track file system changes or user activity. Keywords: Event logs, file system activity, user activity. Open Records Request: Request Windows or Linux event logs from government-operated websites, specifying that you're looking for activity related to file deletions or user actions.

For Self-Hosted Systems: On Windows, check event viewer logs (Event Viewer > Windows Logs > Application/Security). On Linux, system logs are in /var/log/syslog.7. Version Control Logs (if applicable) If your website uses a version control system (e.g., Git), these logs will show when files were modified or deleted.

For Websites Hosted by a Third Party: Request access to the version control logs from your hosting provider or repository management service (e.g., GitHub, GitLab). Keywords: Git logs, version control, file deletions, file modifications. Open Records Request: If a government website uses version control, request the relevant logs, specifying the time period and types of file changes (e.g., additions, deletions).

For Self-Hosted Systems: Access Git logs directly: Instructions: Rungit logo to view a history of commits, showing who made changes and when.

On Wed, Oct 16, 2024 at 7:35 PM Fulton County Georgia wrote:

✉ On 10/16/2024 7:35:01 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**OPEN RECORDS
TELEPHONE (404) 612-0281**

October 16, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, however additional time is needed to fulfill your open records request. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Friday, October 25, 2024. We appreciate your continued patience.

Sincerely,
Mystical Studaway
Paralegal, Open Records Team
County Attorney's Office

✉ On 10/8/2024 5:03:01 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



October 08, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

Also, I am asking for records in regards to the District Attorneys webpage,

<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: We apologize for the delay, additional time is needed to fulfill your open records request. Your request is still in line to be processed by the IT Department. We anticipate an update or response will be forwarded to you within 7 business days or no later than 5:00 p.m. on Thursday, October 17, 2024. We appreciate your continued patience.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
County Attorney's Office

✉ On 10/3/2024 6:14:01 PM, orr@fultoncountyga.gov wrote:

Subject: Fulton County Open Records Center - ORR # R011151-100324:: R011151-100324

Body:



**FULTON
COUNTY**

**OPEN RECORDS
TELEPHONE (404) 612-0281**

October 03, 2024

SENT VIA EMAIL:

Dear Billy Blume:

This correspondence is in response to your Open Records Act Request Reference #: R011151-100324 dated October 03, 2024.

Your request sought the following:

See attached email which is cut and pasted below.

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

A Varonis risk assessment helped this org get their data under control

<https://www.youtube.com/watch?v=2Gi9Iwcil7g>

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

Response: Your request has been submitted to the IT department for processing. We will let you know as soon as we have received an update from them.

Sincerely,

Mystical Studaway
Paralegal, Open Records Team
County Attorney's Office

✉ On 10/3/2024 10:48:39 AM, orr@fultoncountyga.gov wrote:

Dear Billy Blume:

Thank you for submitting an Open Records Request to Fulton County, Georgia.

The County received your Open Records Act request dated October 03, 2024 and has assigned the reference number R011151-100324 for tracking purposes.

Record(s) Requested: *See attached email which is cut and pasted below.*

I am wanting the summary of the scope of the cyber attack that took place Jan 2024. You stated in a video it was internal permissions and employees had access they should not have. It is all internal, so which is it, a internal permissions issue or a cyber attack?

*A Varonis risk assessment helped this org get their data under control
<https://www.youtube.com/watch?v=2Gi9Iwcil7g>*

That video was published Nov 2023.

*Also, I am asking for records in regards to the District Attorneys webpage,
<https://fultoncountyga.gov/districtattorney>, from December 2023 to Sept 2024.*

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study.

Between the dates December 2023 to March 2024 (4 months)

I am requesting these files in Rich text, Text or PDF format as your agency uses PDF software to compile and read documents.

- *Access Logs: These logs record every request made to the server, including what resources (pages, files, etc.) were accessed, who accessed them (IP addresses), and the time of access.*
- *Error Logs: These provide information on any errors encountered by the server, which may include issues related to file deletions or failed access attempts.*
- *Audit Logs: These track any changes made to the database, including deleted entries, altered records, and the user responsible for these changes.*
- *Transaction Logs: This is a sequential record of all database transactions, showing what data was modified or deleted*
- *Security Logs: Track user authentication, permissions changes, and potential security incidents that might relate to deletions*
- *Event Logs: Windows or Linux event logs can track file system and user activity that might indicate deletions*
- *Version Control Logs (if applicable) If the website uses a version control system (e.g., Git), these logs can show when files were added, modified, or deleted and by whom.*
- • •

You may be wondering why you are getting this, well because I can serve a request directly to you and you must fill the request in 72 hours. By law. I will attach the GORA PDF for you to study. If you choose not to fill the request then you, in your individual capacity, can be held accountable for violating the Georgia Open Records laws 50-18-70

You can email me the logs.

*Thank You
Billy Blume*

We will assign the request to the appropriate department(s). If there should be a cost associated with your Open Records Request we will notify you prior to proceeding with the request. If you should have any questions or concerns about your request, please feel free to contact the Fulton County Open Records Team.

Fulton County has an Open Records Center that allows you to submit and track Open Records Act requests. Please click [here](#) to create an account, monitor request progress, and submit future requests.

Sincerely,


Fulton County Open Records Team

E: orr@fultoncountyga.gov

P: (404) 612-0281

Track the issue status and respond at:

https://fultoncountyga.mycusthelp.com/WEBAPP/_rs/RequestEdit.aspx?rid=68019

 On 10/3/2024 10:48:38 AM, orr@fultoncountyga.gov wrote:

Request was created by staff