

Seyfarth Shaw LLP
233 South Wacker
Drive Suite 8000
Chicago, Illinois 60606-
6448 T (312) 460-5000
F (312) 460-7000

scarlson@seyfarth.com

T (312) 460-5946

September 14, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Incident

Dear Sir or Madam:

We represent San Francisco Jazz Organization ("SFJ"), a nonprofit organization dedicated to exploring the full musical spectrum of jazz. SFJ is located at 201 Franklin Street, San Francisco, CA 94102. We are writing to notify you, on behalf of our client, of a data security incident that potentially affected the personal information of residents of Maryland. This notice may be supplemented upon any further investigation. By providing this notice, SFJ does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the relevant state statute, or personal jurisdiction.

Background: SFJ first became aware of a potential security incident on May 23, 2023, when their IT engineering team detected a ransomware attack on their systems. The attackers managed to infiltrate and encrypt several critical components, including file servers, accounting workstations, backups, and backup servers. Immediately upon detecting the intrusion, SFJ launched their incident response protocols to contain and mitigate the situation. SFJ engaged third-party cybersecurity experts on June 1 to conduct a comprehensive forensic investigation. The primary objective was to assess the extent of the breach and determine whether any employee personal information was compromised. The forensic analysis, completed on June 16, revealed that the threat actors may have gained access to database files containing employee personal information. On August 17, 2023, a continued investigation revealed that additional personal information may have been exposed.

This notice is for the same incident. Based on new information, SFJ has chosen to expand the group of individuals that they are notifying.

The personal information that may have been impacted for Maryland residents may include one or more of the following: full name and social security numbers. Additionally, for current and former employees, the information that may have been impacted for Maryland residents may include one or more of the following: driver's license or other government identification numbers, and date of birth.

Upon discovery of the incident, SFJ responded quickly to minimize any impacts. SFJ has begun hardening their systems by installing industry leading countermeasures, such as enhanced encryption, for all sensitive devices. SFJ is also updating security controls on users and their data,

while also implementing two-factor authentication across all of their systems and users. These added layers of security will help prevent unauthorized access to their systems in the future.

Notice to Maryland Residents: We have determined that the number of Maryland residents potentially affected by this security incident is four (4). SFJ will mail notice to impacted individuals on September 15, 2023. Written notice to individuals was provided in substantially the same form as the letter attached here as **Exhibit A**. Please note that we reserve the right to update the draft letter.

Other Steps Taken and To Be Taken: SFJ is taking action to provide assistance to potentially affected individuals, even though it currently has no evidence of any misuse of or fraudulent activity relating to anyone's personal information as a result of this incident. SFJ is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months through Experian at no cost to the individuals.

Additionally, SFJ is providing impacted individuals with guidance on how to better protect against identity theft and fraud. These measures include advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our client is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information: Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at (312) 460-5946 or scarlson@seyfarth.com.

Very truly yours,

SEYFARTH SHAW LLP

/s/ Scott A. Carlson

Scott A. Carlson

SC/dr



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 15, 2023

K0170-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

We are writing to inform you about a recent data security incident that has occurred within our organization. The privacy and security of personal information is very important to us. We want to provide you with all the necessary details a security incident we recently experienced and the steps we are taking to address it.

What Happened: On May 23, 2023, our IT engineering team detected a ransomware attack on our systems. The attackers managed to infiltrate and encrypt several critical components, including file servers, accounting workstations, backups, and backup servers. Immediately upon detecting the intrusion, we launched our incident response protocols to contain and mitigate the situation. We engaged third-party cybersecurity experts on June 1 to conduct a comprehensive forensic investigation.

The primary objective was to assess the extent of the breach and determine whether any employee personal information was compromised. The forensic analysis, completed on June 16, revealed that the threat actors may have gained access to database files containing employee personal information.

On August 17, 2023, we determined that additional personal information may have been exposed. If you have received a notice of an incident from May 2023, this notice is for the same incident. Based on new information, we have expanded the group of individuals that we are notifying.

What Information was Involved: We have investigated the affected systems and identified the following categories of your personal information that may have been accessed by the threat actors:

- Full Name
- Social Security Number
- For Current and Former Employees of SF Jazz:
 - Driver's License or Government Identification Number
 - Date of Birth

We understand that this may be concerning to you, and we apologize for any inconvenience this may have caused. We want to assure you that we are taking every possible step to safeguard your personal information and prevent any further incidents.



What We are Doing to Protect Your Information: We regret that this incident occurred. As a response to the incident, we have taken immediate and comprehensive remedial measures to enhance the security and protection of your data. We are hardening our systems by installing industry leading countermeasures, such as enhanced encryption, for all sensitive devices. We are also fully updating security controls on users and their data, while also implementing two-factor authentication across all of our systems and users. These added layers of security will help prevent unauthorized access to our systems in the future.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** December 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-420-2875 by December 31, 2023. Be prepared to provide engagement number B103627 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-420-2875, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B103627.

What You Can Do: We encourage you to remain vigilant by reviewing your account statements and monitoring credit report information. You can also obtain information about fraud alerts and security freezes from the U.S. Federal Trade Commission (FTC) and the credit reporting agencies listed below:

- Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP

Nationwide Consumer Reporting Companies:

- Equifax, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
- Experian, <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
- TransUnion, <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289

To the extent you desire to freeze your credit report, you must separately place a credit freeze on your credit file at each of the three credit reporting agencies. There is no charge associated with placing a credit freeze. The following information should be included when requesting a credit freeze:

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

For Massachusetts Residents: You have the right to obtain a police report.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

District of Columbia Office of the Attorney General – Office of Consumer Protection; 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; <https://oag.dc.gov/consumer-protection>

Maryland Office of the Attorney General – Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General – Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General – Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Oregon Office of the Attorney General – Consumer Protection Division: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>

Sincerely,

Judy Gum
CFO
SFJAZZ

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000002



Seyfarth Shaw LLP
233 South Wacker
Drive Suite 8000
Chicago, Illinois 60606-
6448 T (312) 460-5000
F (312) 460-7000

scarlson@seyfarth.com

T (312) 460-5946

November 2, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Incident

Dear Sir or Madam:

We represent San Francisco Jazz Organization ("SFJ"), a nonprofit organization dedicated to exploring the full musical spectrum of jazz. SFJ is located at 201 Franklin Street, San Francisco, CA 94102. We are writing to supplement a previous notification to the Office of the Attorney General of Maryland, on behalf of our client, regarding the data security incident that potentially affected the personal information of residents of Maryland. This notice may also be supplemented upon further investigation. By providing this notice, SFJ does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the relevant state statute, or personal jurisdiction.

Background: SFJ first became aware of a potential security incident on May 23, 2023, when their IT engineering team detected a ransomware attack on their systems. The attackers managed to infiltrate and encrypt several critical components, including file servers, accounting workstations, backups, and backup servers. Immediately upon detecting the intrusion, SFJ launched their incident response protocols to contain and mitigate the situation. SFJ engaged third-party cybersecurity experts on June 1 to conduct a comprehensive forensic investigation. The primary objective was to assess the extent of the breach and determine whether any employee personal information was compromised. The forensic analysis, completed on June 16, revealed that the threat actors may have gained access to database files containing employee personal information. On August 17, 2023, a continued investigation revealed that additional personal information may have been exposed.

This notice is for the same incident. Based on new information and continuing analysis, SFJ has chosen to expand the group of individuals that they are notifying.

The personal information that may have been impacted for Maryland residents may include one or more of the following: full name and social security numbers. Additionally, for current and former employees, the information that may have been impacted for Maryland residents may include one or more of the following: driver's license or other government identification numbers, and date of birth.

Upon discovery of the incident, SFJ responded quickly to minimize any impacts. SFJ has begun hardening their systems by installing industry leading countermeasures, such as enhanced

encryption, for all sensitive devices. SFJ is also updating security controls on users and their data, while also implementing two-factor authentication across all of their systems and users. These added layers of security will help prevent unauthorized access to their systems in the future.

Notice to Maryland Residents: We have determined that the number of additional Maryland residents potentially affected by this security incident is one (1). SFJ has mailed notice to impacted individuals on October 25, 2023. Written notice to individuals was provided in substantially the same form as the letter attached here as **Exhibit A**. Please note that we reserve the right to update the draft letter.

Other Steps Taken and To Be Taken: SFJ is taking action to provide assistance to potentially affected individuals, even though it currently has no evidence of any misuse of or fraudulent activity relating to anyone's personal information as a result of this incident. SFJ is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months through Experian at no cost to the individuals.

Additionally, SFJ is providing impacted individuals with guidance on how to better protect against identity theft and fraud. These measures include advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our client is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information: Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at (312) 460-5946 or scarlson@seyfarth.com.

Very truly yours,

SEYFARTH SHAW LLP

/s/ Scott A. Carlson

Scott A. Carlson

SC/us



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 25, 2023



K2292-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L02 SFJAZZ W2

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample,

We are writing to inform you about a recent data security incident that has occurred within our organization. The privacy and security of personal information is very important to us. We want to provide you with all the necessary details a security incident we recently experienced and the steps we are taking to address it.

What Happened: On May 23, 2023, our IT engineering team detected a ransomware attack on our systems. The attackers managed to infiltrate and encrypt several critical components, including file servers, accounting workstations, backups, and backup servers. Immediately upon detecting the intrusion, we launched our incident response protocols to contain and mitigate the situation. We engaged third-party cybersecurity experts on June 1 to conduct a comprehensive forensic investigation.

The primary objective was to assess the extent of the breach and determine whether any employee personal information was compromised. The forensic analysis, completed on June 16, revealed that the threat actors may have gained access to database files containing employee personal information.

On August 17, 2023, we determined that additional personal information may have been exposed. If you have received a notice of an incident from May 2023, this notice is for the same incident. Based on new information, we have expanded the group of individuals that we are notifying.

What Information was Involved: We have investigated the affected systems and identified the following categories of your personal information that may have been accessed by the threat actors:

- Full Name
- Social Security Number

For Current and Former Employees of SF Jazz:

- Driver's License or Government Identification Number
- Date of Birth

We understand that this may be concerning to you, and we apologize for any inconvenience this may have caused. We want to assure you that we are taking every possible step to safeguard your personal information and prevent any further incidents.



What We are Doing to Protect Your Information: We regret that this incident occurred. As a response to the incident, we have taken immediate and comprehensive remedial measures to enhance the security and protection of your data. We are hardening our systems by installing industry leading countermeasures, such as enhanced encryption, for all sensitive devices. We are also fully updating security controls on users and their data, while also implementing two-factor authentication across all of our systems and users. These added layers of security will help prevent unauthorized access to our systems in the future.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by January 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [https:// www.experianidworks.com/credit](https://www.experianidworks.com/credit)
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-420-2875 by January 31, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-420-2875, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

What You Can Do: We encourage you to remain vigilant by reviewing your account statements and monitoring credit report information. You can also obtain information about fraud alerts and security freezes from the U.S. Federal Trade Commission (FTC) and the credit reporting agencies listed below:

- Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP

Nationwide Consumer Reporting Companies:

- Equifax, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
- Experian, <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
- TransUnion, <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289

To the extent you desire to freeze your credit report, you must separately place a credit freeze on your credit file at each of the three credit reporting agencies. There is no charge associated with placing a credit freeze. The following information should be included when requesting a credit freeze:

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

For Massachusetts Residents: You have the right to obtain a police report.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.



Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place, 16th Floor, Baltimore, MD
21202
1-888-743-0023
www.oag.state.md.us

New York Office of Attorney General

Office of the New York State Attorney General
Consumer Frauds & Protection
The Capitol
Albany, NY 12224
1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

Sincerely,

Judy Gum
CFO
SFJAZZ

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.