



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

October 4, 2022

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois represents Reel FX, Inc. ("Reel FX") in connection with a recent data security incident described in greater detail below. Reel FX is a digital animation studio with locations in Dallas, TX, Hollywood, CA, and Montreal, QC. The purpose of this letter is to notify you, in accordance with Me. Rev. Stat. Tit. 10 § 1348, that this incident may have affected the personal information of three (3) Maine residents.

1. Nature of the Security Incident

On June 26, 2022, Reel FX discovered unusual network activity impacting certain systems. Upon discovering this activity, Reel FX took immediate steps to secure its environment and engaged cybersecurity experts to assist with an investigation. The investigation determined that an unknown actor gained access to and may have obtained a limited amount of data from the Reel FX network without authorization between June 4, 2022 and June 26, 2022. Reel FX thereafter undertook a comprehensive review of the potentially affected data to identify any individuals whose sensitive information may have been involved, which concluded on August 24, 2022.

Since that time, Reel FX has been working diligently to identify current contact information needed to notify all individuals potentially affected by this incident. On September 30, 2022, Reel FX identified three (3) Maine residents within the potentially affected population.

2. Type of Information and Number of Maine Residents Affected

Reel FX notified three (3) residents of Maine of this data security incident via first class U.S. mail on October 4, 2022. The type of information involved varied by individual but may have included the Maine residents' names, addresses, dates of birth, bank account and routing numbers, Social Security numbers, and individual taxpayer identification numbers. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as Reel FX discovered this incident, it took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Reel FX has also implemented additional security features to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

Reel FX has established a toll-free call center through Kroll to answer questions about the incident and address related concerns. In addition, Reel FX is offering twelve months of complimentary credit and identity monitoring services to all potentially affected individuals.

4. Contact Information

Reel FX remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at Lindsay.Nickle@lewisbrisbois.com. Please let me know if you have any questions.

Sincerely,



Lindsay B. Nickle
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN

Attachment: Consumer Notification Letter Template



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (“Re: Notice of Data” [Breach/Incident])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have affected your personal information. Reel FX, Inc. and Reel FX Creative Studios, Inc. (“Reel FX”) takes the privacy and security of your personal information very seriously. This is why we are informing you of this incident, providing you with steps you can take to help protect your personal information, and offering you complimentary twelve (12) months of identity monitoring services.

What Happened: On June 26, 2022, Reel FX discovered unusual network activity impacting certain systems. We immediately took steps to secure our environment and engaged cybersecurity forensic experts to assist us with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the Reel FX network without authorization between June 4, 2022 and June 26, 2022.

The good news is that our cybersecurity forensic experts were successful in containing the event. However, following a thorough review of the impacted information, on August 24, 2022, we determined that some of your personal information may have been involved in the incident. Since that time, Reel FX has worked diligently to identify current contact information needed to notify all potentially affected individuals. We currently have no reason to believe your information was misused as a result of this incident. If you are receiving this letter, you may currently be, or have been, employed by Reel FX or one of its sister companies (including those under the “Bedrock” umbrella of companies).

What Information Was Involved: The information affected may have included your name and contact information (such as your address or phone number), date of birth, bank account and routing number, Social Security Number, or Individual Taxpayer Identification Number.

What We Are Doing: As soon as Reel FX discovered the incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. Furthermore, we reported the incident to the Federal Bureau of Investigation, the Canadian Anti-Fraud Centre, the Royal Canadian Mounted Police, and the Office of the Privacy Commissioner of Canada and will provide whatever cooperation is necessary to help identify and prosecute the perpetrators. While we have no indication that your information has been misused, we are nonetheless providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you complimentary identity monitoring services for twelve (12) months through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The Kroll services, which are free to you upon activation, include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your offer for identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to help protect your information. In addition, we encourage you to activate in the identity monitoring services we are offering through Kroll.

For More Information: If you have questions or need assistance, please call (855) 926-1130, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Representatives are fully versed on this incident and can help answer questions you may have regarding the identity monitoring of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Steve O'Brien', with a long horizontal flourish extending to the right.

Steve O'Brien

CEO

Reel FX, Inc. and Reel FX Creative Studios, Inc.

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (“Re: Notice of Data” [Breach/Incident])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have affected your personal information. Reel FX, Inc. and Reel FX Creative Studios, Inc. (“Reel FX”) takes the privacy and security of your personal information very seriously. This is why we are informing you of this incident, providing you with steps you can take to help protect your personal information, and offering you twelve (12) months of complimentary identity monitoring services.

What Happened: On June 26, 2022, Reel FX discovered unusual network activity impacting certain systems. We immediately took steps to secure our environment and engaged cybersecurity forensic experts to assist us with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the Reel FX network without authorization between June 4, 2022 and June 26, 2022.

The good news is that our cybersecurity forensic experts were successful in containing the event. However, following a thorough review of the impacted information, on August 24, 2022, we determined that some of your personal information may have been involved in the incident. Since that time, Reel FX has worked diligently to identify current contact information needed to notify all potentially affected individuals. We currently have no reason to believe your information was misused as a result of this incident. If you are receiving this letter, you may have performed work for Reel FX or one of its sister companies (including those under the “Bedrock” umbrella of companies).

What Information Was Involved: The information affected may have included your name and contact information (such as your address or phone number), date of birth, bank account and routing number, Social Security Number, or Individual Taxpayer Identification Number.

What We Are Doing: As soon as Reel FX discovered the incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. Furthermore, we reported the incident to the Federal Bureau of Investigation, the Canadian Anti-Fraud Centre, the Royal Canadian Mounted Police, and the Office of the Privacy Commissioner of Canada and will provide whatever cooperation is necessary to help identify and prosecute the perpetrators. While we have no indication that your information has been misused, we are nonetheless providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you complimentary identity monitoring services for twelve (12) months through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The Kroll services, which are free to you upon activation, include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your offer for identity monitoring services.

You have until <<b2b_text_6 (date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to help protect your information. In addition, we encourage you to activate in the identity monitoring services we are offering through Kroll.

For More Information: If you have questions or need assistance, please call (855) 926-1130, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Representatives are fully versed on this incident and can help answer questions you may have regarding the identity monitoring of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve O'Brien", with a long horizontal flourish extending to the right.

Steve O'Brien

CEO

Reel FX, Inc. and Reel FX Creative Studios, Inc.

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.