Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

We are writing to notify you of a data security incident involving some of your information that occurred at Financial Business and Consumer Solutions (FBCS), a third party service provider previously used by Comcast. Although FBCS experienced the security incident, we are taking initiative to support any former and present customers who have been impacted. This notice explains the incident, measures we have taken and some steps you can take in response.

What Happened? On March 13, 2024, FBCS notified Comcast that it had experienced a data breach incident, but that Comcast consumer data was not impacted. However, on July 17, 2024, FBCS notified Comcast of its new finding that Comcast data was impacted. FBCS provided the following information: "[f]rom February 14 and February 26, 2024, an unauthorized party gained access to FBCS's computer network and some of its computers. During this time, the unauthorized party downloaded data from FBCS systems and encrypted some systems as part of a ransomware attack. Upon discovering the attack on February 26, 204, FBCS launched an investigation with the assistance of third-party cybersecurity specialists. In the course of that investigation, FBCS discovered that the files downloaded by the unauthorized party contained personal information, including personal information about you. FBCS also notified the Federal Bureau of Investigation (FBI) of this attack."

This security incident occurred entirely at FBCS and not at Xfinity or on Comcast systems. FBCS notified Comcast that due to its current financial status, it would no longer able to provide notices or credit monitoring protection to individuals impacted by the incident. As such, we are contacting you directly and providing support services. FBCS received your information because they previously provided Comcast with collections-related services for delinquent payments until 2020, when Comcast ceased working with FBCS. The compromised information about you dates from around 2021, as FBCS is subject to data retention requirements beyond Comcast's working relationship with FBCS.

What Information Was Involved? FBCS's investigation discovered that files downloaded by the unauthorized party included your name, address, Social Security number, date of birth, and your Comcast account number and ID numbers used internally at FBCS. FBCS states that it has no indication that any personal information compromised during this incident has been further misused.

What We Are Doing. We are offering you complimentary identity theft protection services for at least 12 months through membership in CyEx Identity Defense Complete, which includes credit monitoring services. Since FBCS informed Comcast of this incident on July 17, 2024, Comcast has been working with FBCS to understand how the incident occurred and to notify affected individuals (including you) and appropriate governmental authorities. As stated above, Comcast no longer uses FBCS. Notifications about this incident have not been delayed due to law enforcement investigation.

What You Can Do. In addition to enrolling in the identify theft protection services referenced above at no cost to you, we encourage you (as we always encourage all our customers) to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. Please review the "Additional Steps You Can Take" information enclosed with this letter. We also encourage all of our customers to better protect their Xfinity accounts by signing up for two-step verification.[1] All customers should remain alert for unusual or suspicious emails or telephone calls. Information about common scams and how to protect yourself and your Xfinity account are available on our website.[2]

For More Information. We sincerely regret any inconvenience caused by this incident. If you have any questions, please call 888-769-8426, Monday through Friday, between 9:00 am and 9:00 pm, Eastern Time, Monday through Friday.

Sincerely,

Comcast

[1] Learn more at https://www.xfinity.com/support/articles/two-step-verification-xfinity-app-setup
[2] https://www.xfinity.com/support/articles/protect-yourself-phone-scams

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

- **Additional Free Resources on Identity Theft**: You can obtain information from the consumer reporting agencies, the FTC (https://www.identitytheft.gov/) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. Below is the contact information for the Attorneys General for residents of New York, North Carolina, Rhode Island, Oregon, the District of Columbia, and Maryland.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
https://ag.ny.gov/
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
401-274-4400

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
https://www.doj.state.or.us/consumer-protection/
1-877-877-9392

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
https://oag.dc.gov/

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses listed above.

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Comcast Corporation, 1701 John F. Kennedy Boulevard, Philadelphia, PA 19103, 888-769-8426.

Identity Defense

<<Full Name>>
Enter your Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term:<<12/24>> Months*

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit {{URL}}

1. Enter your unique Activation Code **<<Activation Code>>**
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.