

Jena M. Valdetero
Tel 312.456.1025
Fax 312.456.8435
Jena.valdetero@gtlaw.com

October 31, 2024

Attorney General Anthony G. Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notification of Security Incident

Dear Attorney General Brown:

We are writing to inform you that our client, SelectBlinds, is notifying approximately 3,403 residents of a data security incident that may have impacted some of their personal information.

On September 28, 2024, SelectBlinds observed unusual activity on its website and immediately began investigating with the assistance of leading third-party external security experts who discovered that an unauthorized party installed malware on the check-out page on www.selectblinds.com on January 7, 2024. Following a thorough investigation that was completed on October 10, 2024, we determined personal information belonging to some SelectBlinds customers was subject to unauthorized access.

The information affected by the scraping malware includes name, email, shipping and billing addresses, and phone number, payment card information, including card number, expiration date, and security (CVV) code and, for a subset of individuals, potentially their username and password for www.selectblinds.com. SelectBlinds has no indication that any personal information has been misused as a result of the incident.

SelectBlinds takes the security of personal information very seriously and has taken steps to prevent a reoccurrence by increasing the monitoring of its networks, further improving security controls, and hardening its systems. In addition, SelectBlinds has temporarily locked user accounts on its website which will require customers to reset their passwords the next time they attempt to log in. SelectBlinds has notified and is cooperating with federal law enforcement authorities.

SelectBlinds mailed the attached notification to all potentially affected individuals beginning October 31, 2024. The three major Credit Reporting Agencies are also being notified. We have

Office of the Attorney General

October 31, 2024

Page 2

also advised our customers to take precautionary measures on any other online accounts, such as changing their passwords and monitoring their other accounts for any suspicious activity.

Please contact me for any additional information.

Best Regards,

A handwritten signature in blue ink that reads "Jena Valdetero". The signature is fluid and cursive, with the first name "Jena" and last name "Valdetero" clearly legible.

Jena Valdetero

Shareholder

JMV:

Schedule A
Individual Notification Letters



RE: Notice of Data Breach
Please read this entire letter

Dear [REDACTED],

We write to inform you of a data security incident that may have impacted some of your personal information. SelectBlinds is an online retailer that offers custom window coverings. We are notifying you of a recent security incident involving the username and password that you use to access your account on the SelectBlinds website. We take the security of your personal information very seriously, and we sincerely regret having to share this news with you.

Beginning on or about January 7, 2024, an unauthorized third party embedded malware on the SelectBlinds website that allowed data scraping on logins on the check-out page. We became aware of the incident on September 28, 2024, and, following our incident response process, immediately launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. We completed our investigation on October 10, 2024. Through our investigation, we learned that your www.selectblinds.com username and password was affected if you logged in to the check-out page only on the SelectBlinds website while making or considering a purchase.

SelectBlinds takes the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a recurrence. We quickly contained the incident and eradicated the malware and elements of unauthorized access. Among other actions, we have increased monitoring, further improved security controls, and reinforced our systems. In addition, out of an abundance of caution, we have temporarily locked your www.selectblinds.com user account. The next time you go to log in, you will be prompted to securely change your password.

We recommend that you review the additional information below, which contains other important steps you can take to protect your personal information. We also encourage you to change your passwords on any online accounts where the same log-in credentials are used and to monitor such accounts for unauthorized activity.

If you would like to request any additional information about this incident, please contact us at 1-866-586-7032. Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

SelectBlinds

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission for more information on preventing identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit

https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 815 Rhode Island residents notified in this incident.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Attorney General
400 6th Street NW Washington, DC 20001 1-202-442-9828 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

This email was sent by: IDX to [REDACTED]
10300 SW Greenburg Road Suite 570, Portland, OR, 97223 US

[Privacy Policy](#)

Click here to [unsubscribe](#)





P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 31, 2024

RE: Notice of Data Breach
Please read this entire letter

Dear <<First Name>> <<Last Name>>:

We write to inform you of a data security incident that may have impacted some of your personal information. SelectBlinds is an online retailer that offers custom window coverings. We take the security of your personal information very seriously, and we sincerely regret having to share this news with you. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?

Beginning on or about January 7, 2024, an unauthorized third party embedded malware on the SelectBlinds website that allowed data scraping on sales transactions that were entered on the check-out page. We became aware of the incident on September 28, 2024, and, following our incident response process, immediately launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. We completed our investigation on October 10, 2024.

What Information Was Involved?

Through our investigation, we learned that certain data may have been accessed and obtained without authorization by a third party. This data includes your name, email, shipping and billing addresses, and phone number, along with your payment card information, including card number, expiration date, and security (CVV) code. Your www.selectblinds.com username and password may also have been affected if you logged in to the check-out page only on the SelectBlinds website while making a purchase.

What We Are Doing

SelectBlinds takes the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence. We quickly contained the incident and eradicated the malware and elements of unauthorized access. Among other actions, we have increased monitoring, further improved security controls, and reinforced our systems. In addition, out of an abundance of caution, we have temporarily locked your www.selectblinds.com user account. The next time you go to log in, you will be prompted to securely change your password.

What You Can Do

We recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information. We also encourage you to change your passwords on any online accounts where the same log-in credentials are used and to monitor such accounts for unauthorized activity. You should review your payment card statements for any unauthorized charges and report those charges to your credit card issuer. Federal law limits a cardholder's liability in the event of credit card fraud.

For More Information

If you would like to request any additional information about this incident, please contact us at 1-866-586-7032. Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

SelectBlinds

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission for more information on preventing identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 815 Rhode Island residents notified in this incident.

DC Attorney General
400 6th Street NW
Washington, DC
20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
<https://www.marylandattorneygeneral.gov/>

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
<https://ncdoj.gov/>

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 31, 2024

RE: Notice of Data Breach
Please read this entire letter

Dear <<First Name>> <<Last Name>>:

We write to inform you of a data security incident that may have impacted some of your personal information. SelectBlinds is an online retailer that offers custom window coverings. We take the security of your personal information very seriously, and we sincerely regret having to share this news with you. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?

Beginning on or about January 7, 2024, an unauthorized third party embedded malware on the SelectBlinds website that allowed data scraping on sales transactions that were entered on the check-out page. We became aware of the incident on September 28, 2024, and, following our incident response process, immediately launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. We completed our investigation on October 10, 2024.

What Information Was Involved?

Through our investigation, we learned that certain data may have been accessed and obtained without authorization by a third party. This data includes your name, email, shipping and billing addresses, and phone number, along with your payment card information, including card number, expiration date, and security (CVV) code.

What We Are Doing

SelectBlinds takes the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence. We quickly contained the incident and eradicated the malware and elements of unauthorized access. Among other actions, we have increased monitoring, further improved security controls, and reinforced our systems. In addition, out of an abundance of caution, if you have a user account on www.selectblinds.com, we have temporarily locked your account. The next time you go to log in, you will be prompted to securely change your password.

What You Can Do

We recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information. You should review your payment card statements for any unauthorized charges and report those charges to your credit card issuer. Federal law limits a cardholder's liability in the event of credit card fraud.

For More Information

If you would like to request any additional information about this incident, please contact us at 1-866-586-7032. Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

SelectBlinds

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission for more information on preventing identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud_center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze_center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 815 Rhode Island residents notified in this incident.

DC Attorney General

400 6th Street NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General

200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
<https://www.marylandattorneygeneral.gov/>

New York Attorney General

120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General

9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
<https://ncdoj.gov/>

Rhode Island Attorney General

150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov