

MATTHEW J. PLATKIN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street – 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for Plaintiffs

FILED

May 18 2022

Division of Consumer Affairs

By: Cody I. Valdez (278232019)
Deputy Attorney General

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC
SAFETY
DIVISION OF CONSUMER AFFAIRS

In the Matter of

WEICHERT CO. AND ITS AFFILIATES,

Respondent.

Administrative Action

CONSENT ORDER

WHEREAS this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection (“Division”), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -227 (“CFA”), the New Jersey Identity Theft Protection Act, N.J.S.A. 56:8-161 to -166.3 (“ITPA”), and Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 to -6809 & 15 U.S.C. §§ 6821 -6827 (“GLBA”), have been or are being committed (the “Investigation”) by Weichert Co. on behalf of itself and certain of its Affiliates (“Weichert”);

WHEREAS the Attorney General is charged with the responsibility of enforcing the CFA and the ITPA, and the Director of the Division is charged with administering the CFA on behalf of the Attorney General;

WHEREAS Weichert is a family of full-service real estate and financial companies with its corporate headquarters in Morris Plains, New Jersey;

WHEREAS the Division alleges that Weichert engaged in conduct in violation of the CFA and ITPA in connection with its (1) representations of compliance with the GLBA, and (2) unreasonable security measures implemented to secure Personal Information and Nonpublic Personal Information stored on its workstations and servers that lead to data breaches that affected 10,926 consumers and employees, including 6,949 New Jersey residents; and

WHEREAS the Division and Weichert (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and Weichert having cooperated with the Investigation and consented to the entry of the within order (“Consent Order”) without admitting any violation of law, and for good cause shown:

IT IS SO ORDERED AND AGREED as follows:

1. EFFECTIVE DATE

1.1 This Consent Order is effective on the date that it is filed with the Division, which filing date the Division Clerk stamps on the executed Consent Order (“Effective Date”).

2. DEFINITIONS

As used in this Consent Order, the following words or terms shall have the following meanings, which shall apply wherever the words or terms appear in this Consent Order:

2.1 “Affiliate[s]” means any Entity directly or indirectly owned by Weichert, any Person or Entity directly or indirectly controlled by Weichert, any Person or Entity that directly or indirectly controls Weichert, and any officer, director, partner, copartner, employee or agent of such Person or Entity.

2.2 “Attorney General” shall refer to the Attorney General of the State of New Jersey

and the Office of the Attorney General of the State of New Jersey.

2.3 “Consumer Fraud Act” or “CFA” refers to N.J.S.A. 56:8-1 to -226.

2.4 “Controlling Interest” shall be defined as the holding of a majority interest or any degree of ownership of a business sufficient to give the holder the means of exercising control over the management or operations of the business.

2.5 “Cyber Security Operations Center” or “C-SOC” shall mean the employment of person(s), processes, and technology to continuously monitor and update Weichert’s security posture while preventing, detecting, and analyzing and responding to Security Incidents.

2.6 “Data Breach 1” refers to the compromise of consumer Personal Information resulting from the unauthorized backdoor installed on Weichert’s FTP Server from July 2016 to December 2017, which Weichert notified the New Jersey State Police and consumers about on June 11, 2018.

2.7 “Data Breach 2” refers to the compromise of consumer Personal Information resulting from the unauthorized access to 16 employee email accounts occurring between November 7, 2017 and December 20, 2017, which Weichert notified the New Jersey State Police and consumers about on August 5, 2019.

2.8 “Data Breach 3” refers to the compromise of consumer Personal Information resulting from the unauthorized access to 12 employee email accounts occurring between May 25, 2018 and July 26, 2018, which Weichert notified the New Jersey State Police and consumers about on September 20, 2019.

2.9 “Data Breaches” refers collectively to Data Breach 1, Data Breach 2, and Data Breach 3.

2.10 “Encrypt,” “Encrypted,” or “Encryption” shall refer to the transformation of data at rest or in transit into a form in which meaning cannot be assigned without the use of a

confidential process or key. The manner of Encryption shall conform to existing industry standard, which applies to what the standard may become as the industry changes over time. As of the Effective Date, the existing industry standard shall be defined pursuant to Federal Information Processing Standards Publication 140-3.

2.11 “Entity” means any business entity, including but not limited to a partnership, corporation, limited liability company or corporation, trust, estate, incorporated or unincorporated association, any governmental agency or Entity, and any other legal or commercial Entity however organized.

2.12 “Financial Institution” shall be defined in accordance with 15 U.S.C. § 6809(3).

2.13 “Gramm-Leach-Bliley Act” or “GLBA” refers to 15 U.S.C. §§6801 to -6809 & 15 U.S.C. §§6821 to -6827, and applicable federal rules promulgated by the Federal Deposit Insurance Corporation, 12 C.F.R. Part 332, Consumer Financial Protection Bureau, 12 C.F.R. Part 1016, and the Federal Trade Commission, 16 C.F.R. Parts 313 and 314.

2.14 “Identity Theft Protection Act” or “ITPA” refers to N.J.S.A. 56:8-161 to -166.3.

2.15 “Information System[s]” shall be defined in accordance with 16 C.F.R. § 314.2(j) of the Electronic Code of Federal Regulations.

2.16 “Multi-factor Authentication” means authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password; (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone, or (iii) inherent factors, such as biometric characteristics.

2.17 “New Jersey” or “State” refers to the State of New Jersey.

2.18 “Nonpublic Personal Information” or “NPI” shall be defined in accordance with 15 U.S.C. § 6809(4).

2.19 “Open Public Records Act” refers to N.J.S.A. 47:1A-1 to -13.

2.20 “Person[s]” means any natural person or individual.

2.21 “Personal Information” or “PI” shall be defined in accordance with N.J.S.A. 56:8-161.

2.22 “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System.

2.23 “Server” refers to the physical computing device(s) used by Weichert to process, store and/or communicate data by and between multiple devices.

2.24 “Third-Party Assessor” refers to an individual qualified as a Certified Information Systems Auditor or as a Certified Information Systems Security Professional and who has at least five years of experience evaluating the effectiveness of information system security or computer networks of Financial Institutions.

2.25 “Weichert” refers to a family of full-service real estate and financial companies that is comprised of real estate brokerage and related mortgage financing, homeowners’ insurance and title insurance services, including, but not limited to Weichert Co. d/b/a Weichert Realtors, Mortgage Access Corp. d/b/a Weichert Financial Services, Weichert Insurance Agency, Inc., and Title Closing Services LLC d/b/a Weichert Title Agency d/b/a Democracy Title Agency, and their successors and Affiliates.

2.26 “Weichert Network” shall mean the networking equipment, databases or data stores, applications, Servers, workstations, and endpoints that are capable of using or sharing software, data, and hardware resources and that are licensed services, owned and/or operated by Weichert.

3. STIPULATED FACTS

3.1 On or about December 20, 2017, Weichert discovered Breach 1 when it identified an unauthorized backdoor on Weichert's FTP Server. After completing its investigations, Weichert identified the names and addresses of affected individuals whose PII was stored in the FTP server from February 7, 2018, to March 6, 2018. Weichert notified the affected individuals and the New Jersey State Police of Data Breach 1 on June 11, 2018.

3.2 At the time of Data Breach 1, Weichert's FTP Server contained records with the Personal Information of at least 3,553 consumers, including 1,965 New Jersey residents. The information in these records included names, addresses, Social Security numbers, credit card information, driver's license numbers, other government identification numbers, and payroll deductions.

3.3 Data Breach 1 affected some Weichert Entities, including Mortgage Access Corp. and Weichert Insurance Agency, Inc.

3.4 On or about December 20, 2017, Weichert discovered Breach 2 when it identified that several employee email accounts were subject to a business email compromise. On August 5, 2019, after completing its investigations and identifying the names and addresses of the individuals affected by Breach 2, Weichert disclosed Data Breach 2 to consumers and the New Jersey State Police. Data Breach 2 resulted in the compromise of the PI of at least 6,423 consumers, including 4,136 New Jersey residents.

3.5 The information affected by the business email compromise that resulted in Data Breach 2 included names, addresses, Social Security numbers, passport numbers or government issued identification numbers, payment card numbers, and financial account numbers.

3.6 Data Breach 2 affected some Weichert Entities, including Mortgage Access Corp and Title Closing Services, LLC.

3.7 On or about July 3, 2018, Weichert discovered Breach 3, another business email compromise, while it was investigating Breach 2. After completing its investigation and identifying the names and addresses of the affected individuals, on September 20, 2019, Weichert disclosed Data Breach 3 to consumers and the New Jersey State Police. Data Breach 3 resulted in the compromise of the Personal Information of approximately 1,100 consumers, including 863 New Jersey residents.

3.8 The business email compromise resulting in Data Breach 3 involved names, addresses, driver's license numbers, passport numbers, payment card numbers, and financial account numbers.

3.9 Data Breach 3 affected some Weichert Entities, including Mortgage Access Corp.

3.10 Certain Weichert Entities affected by the Data Breaches are subject to the requirements of the GLBA as Financial Institutions.

4. ALLEGED VIOLATIONS OF LAW

4.1 The Division has alleged the following:

- a. At all relevant times set forth in Section 3 above (the "Relevant Time Period"), incorporated herein by reference, Mortgage Access Corp., and Weichert Insurance Agency, Inc., and Title Closing Services, LLC were and continue to be Financial Institutions.
- b. As Financial Institutions, Mortgage Access Corp., Weichert Insurance Agency, Inc., Title Closing Services, LLC, and the Affiliates with whom Mortgage Access Corp., Weichert Insurance Agency Inc., and Title Closing Services, LLC share NPI were, and continue to be, required to comply with the GLBA.
- c. Mortgage Access Corp., Weichert Insurance Agency, Inc., Title Closing Services, LLC and the Affiliates with whom Mortgage Access Corp., Weichert Insurance

Agency Inc., and Title Closing Services, LLC shared NPI violated the CFA when they failed to implement adequate security measures to comply with the GLBA.

d. Specifically, Weichert, as the owner and operator of the Weichert Network, and on behalf of Mortgage Access Corp., Weichert Insurance Agency, Inc., Title Closing Services, LLC, and the Affiliates with whom Mortgage Access Corp., Weichert Insurance Agency Inc., and Title Closing Services, LLC shared NPI, failed to comply with the GLBA by:

- i. Failing to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the complexity, nature and scope of the activities conducted by Weichert, and the sensitivity of any customer information at issue, in violation of 16 C.F.R. § 314.3(a) (effective until January 10, 2022);
- ii. Failing to identify reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and failing to assess the sufficiency of any safeguards in place to control these risks, in violation of 16 C.F.R. § 314.4(b) (effective until January 10, 2022);
- iii. Failing to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, in violation of 16 C.F.R. § 314.4(c) (effective until January 10, 2022); and

- iv. Failing to evaluate and adjust the information security program in light of the results of the testing and monitoring required by 16 C.F.R. § 314.4(c); any material changes to operations or business arrangements; or any other circumstances that are known or have reason to be known that may have a material impact on the information security program, in violation of 16 C.F.R. § 314.4(e) (effective until January 10, 2022).
- e. At all relevant times, Weichert offered for sale and sold services that are merchandise and real estate within the meaning of the CFA.
- f. Weichert violated the CFA by not restricting access to information only to those employees for whom access is appropriate, in violation of N.J.S.A. 56:8-2.
- g. Weichert violated the CFA by not protecting the PI of its customers, some of whom are New Jersey residents, with the utmost degree of confidentiality, in violation of N.J.S.A. 56:8-2.
- h. At all relevant times, Weichert conducted business in New Jersey and collected PI from New Jersey residents within the meaning of the ITPA.
- i. Weichert violated the ITPA by failing to disclose Breach 1 in the most expedient time possible and without unreasonable delay to: (i) customers, (ii) The New Jersey State Police, and (iii) Consumer Reporting Agencies, in violation of N.J.S.A. 56:8-163(a), N.J.S.A. 56:8-163(c)1, and N.J.S.A. 56:8-163(f).
- j. Weichert violated the ITPA by failing to disclose Breach 2 in the most expedient time possible and without unreasonable delay to: (i) customers, (ii) The New Jersey State Police, and (iii) Consumer Reporting Agencies, in violation of N.J.S.A. 56:8-163(a), N.J.S.A. 56:8-163(c)1, and N.J.S.A. 56:8-163(f).

- k. Weichert violated the ITPA by failing to disclose Breach 3 in the most expedient time possible and without unreasonable delay to: (i) customers, (ii) The New Jersey State Police, and (iii) Consumer Reporting Agencies, in violation of N.J.S.A. 56:8-163(a), N.J.S.A. 56:8-163(c)1, and N.J.S.A. 56:8-163(f).
- l. Weichert violated the ITPA by failing to notify the New Jersey State Police of the additional 111 individuals affected by Breach 3, determined after the initial notification to the New Jersey State Police was made, in violation of N.J.S.A. 56:8-163(c)(1).

4.2 The Division has alleged that Weichert's conduct described in Paragraph 4.1 constitute separate and additional unconscionable commercial practices in violation of the CFA, N.J.S.A. 56:8-2.

4.3 Weichert disputes the allegations set forth in Paragraphs 4.1 and 4.2.

5. SETTLEMENT PAYMENT

5.1 The Parties have agreed to a monetary settlement pursuant to this Final Consent Judgment in the amount of \$1,200,000.00 ("Settlement Payment"), to be paid to the Division within sixty (60) days of the Effective Date. This Settlement Payment consists of \$1,074,350.00 allocated to the Division's civil penalty claims, and \$125,650.00 allocated to the Division's claims for reimbursement of attorneys' fees and investigative costs. The Settlement Payment is not a finding by the Division or admission by Weichert of liability.

5.2 Weichert shall make the Settlement Payment by wire transfer, credit card, or by certified check, cashier's check or money order made payable to the "New Jersey Division of Consumer Affairs" and forwarded to:

Case Initiation and Tracking Unit
New Jersey Department of Law and Public Safety
Division of Consumer Affairs

124 Halsey Street – 7th Floor
P.O Box 45025
Newark, New Jersey 07101
Attention: Van Mallett, Lead Investigator

5.3 Upon making the Settlement Payment, Weichert shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the Division pursuant to the terms herein.

6. INJUNCTIVE RELIEF

I. Compliance with State and Federal Laws

6.1 Weichert shall comply with the CFA, ITPA, and GLBA to the extent each are applicable, in connection with its collection, maintenance, and safeguarding of PI and NPI from any future breach of security. As part of compliance with the CFA, Weichert shall not make any misrepresentations to consumers about the extent to which Weichert maintains the privacy, security, and confidentiality of PI or NPI.

6.2 If a Security Incident does not qualify as a breach requiring notification, Weichert shall create a report that includes a description of the Security Incident and the response to that Security Incident (“Security Incident Report”). The Security Incident Report shall be made available for inspection by the Third-Party Assessor, as described herein.

II. Information Security Program

6.3 Weichert shall continue to develop, implement, and maintain a written information security program (“Information Security Program” or “Program”) that is reasonably designed to protect the security, integrity, and confidentiality of the PI and NPI that it collects, stores, transmits, and/or maintains. At a minimum, the Program shall continue to include the information security requirements in Paragraphs 6.4 and 6.5 below.

a. As discussed here, the Program shall comply with any applicable requirements under State or federal law, and shall contain administrative, technical, and physical safeguards appropriate to (i) the size and complexity of the business; (ii) the nature and scope of Weichert's activities, and (iii) the sensitivity of the PI and NPI that Weichert collects, stores, transmits, and/or maintains.

b. Weichert may satisfy the requirements of this Consent Order, including the implementation of the Information Security Program through the review, maintenance, and if necessary, updating of its existing information security program and existing safeguards, provided that such existing program and safeguards meet the requirements set forth in this Consent Order.

c. Weichert shall review not less than annually the Information Security Program.

d. The Program shall require Weichert to continue to maintain an appointed qualified individual as Chief Information Security Officer ("CISO") with the responsibility to implement, maintain, enforce, and monitor the Program. The CISO shall have appropriate training, experience, and expertise in the field of information security to oversee the Program.

e. The role of the CISO will include regular and direct reporting to the Chief Operating Officer and Chief Financial Officer of Weichert regarding the status of the Program, the security risks faced, resources required for implementation of the Program, and the security implications of Weichert's business decisions. At minimum, the CISO shall provide a written report to the Chief Operating Officer and Chief Financial Officer of Weichert on at least a quarterly basis, and to the Board of Directors on a semi-annual basis. The CISO shall report to Weichert's Chief Operating Officer and Chief Financial Officer within twenty-four (24) hours of a confirmed Security Incident impacting 500 or more consumers residing in the United States for a period of seven (7) years from the Effective Date.

f. Weichert shall provide notice of the requirements of this Consent Order to the management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement training to those employees on the requirements of this Consent Order. Weichert shall provide the training required under this paragraph to the employees Weichert within one hundred twenty (120) days of the Effective Date of this Consent Order or prior to their handling of any PI or NPI.

g. As part of its Information Security Program, Weichert shall develop, implement, and maintain a documented written incident response plan to prepare for and respond to any future Security Incident. Weichert shall revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI and NPI. At a minimum, this plan shall provide for the following phases of a response: Preparation; Detection and Analysis; Containment; Notification and Coordination with Law Enforcement and Regulators; Recovery; Consumer Notification and Remediation; and Post-Incident Analysis.

h. Weichert shall ensure that its Information Security Program receives the resources and support reasonably necessary to function as needed.

III. *Specific Information Security Requirements*

6.4 At minimum the Program's administrative, technical, and physical safeguards must include:

a. Data Collection & Retention: Weichert shall continue to develop, implement, and maintain reasonable policies and procedures governing its collection, use, and retention of PI and NPI, including data classification policies and associated handling procedures.

b. Device Identification and Management: Weichert shall continue to identify and manage the data, personnel, devices, systems, and facilities that enable Weichert to achieve its business purposes in accordance with their relative importance to business objectives.

c. Asset Inventory: Weichert shall continue to develop, maintain, and regularly update a reasonable inventory of the assets that primarily comprise the Weichert Network, and appropriately identify and secure assets containing PI and NPI.

d. Cyber Security Operations Center: Weichert shall continue to maintain the existence and operation of a C-SOC, or third-party IT vendor that performs services reasonably equivalent to a C-SOC. The C-SOC or reasonably equivalent third-party IT vendor shall provide comprehensive monitoring of Servers and other technologies to identify improper use of data, including PI and NPI. The C-SOC or reasonably equivalent third-party IT vendor's analytic capabilities shall be deployed to detect, analyze, and respond to potential and confirmed Security Incidents.

e. Encryption: Weichert shall continue to protect by Encryption all customer information held or transmitted by Weichert both in transit over external networks and at rest. To the extent that Encryption of customer information, either in transit over external networks or at rest, is infeasible, Weichert may instead secure such customer information using effective alternative compensating controls reviewed and approved by its CISO.

f. Antivirus Maintenance: Weichert shall continue to maintain current, up-to-date antivirus protection programs, or reasonably equivalent technology, on all Information Systems connected to the Weichert Network.

g. Authentication: Weichert shall continue to maintain reasonable policies and procedures that authenticate and permit access only to authorized users and protect against unauthorized access to PI and NPI stored and maintained by Weichert, and limit authorized employees' access to only the PI and NPI that they need to perform their duties and functions. Such policies shall continue to have updates implemented as reasonably necessary.

h. Access Controls: Weichert shall continue to implement and maintain appropriate controls to manage access and use of all accounts with access to PI or NPI, including individual accounts, administrator accounts, services accounts, and vendor accounts. Such controls shall include a means to regularly review access and access levels of users and remove network and remote access at the time of notification of termination for any employee whose employment has ended or any non-associate whose term has ended.

i. Multi-factor Authentication: Weichert shall continue to implement and maintain Multi-factor Authentication for any individual accessing any Information System connected to the Weichert Network, including employee email accounts and remote access to the Weichert Network, unless the CISO has approved in writing the use of a reasonably equivalent or more secure alternative.

j. Administrators/Non-administrators: Weichert shall continue to implement and maintain reasonable policies and procedures to determine which employees require administrator privileges to perform their duties and functions, and restrict employees that do not require administrator privileges from downloading or running any unauthorized software.

k. Passwords: Weichert shall continue to implement and maintain a password policy that at a minimum requires: (i) passwords for all employees of Weichert to expire and be reset every six (6) months; (ii) a password to access each device connected to the Weichert Network; (iii) default passwords to be changed to unique passwords; and (iv) a reasonably up-to-date password hashing technology.

l. Software Updates: Weichert shall continue to update all Information Systems connected to the Weichert Network with critical security updates within thirty (30) days of the updates becoming available, unless Weichert's CISO has determined in writing that the critical security update will adversely affect the security of the Weichert Network.

m. Risk Assessments: Weichert shall continue to develop, implement, and maintain a risk assessment program to identify, address, and as appropriate, remediate risks affecting the Weichert Network. At minimum, Weichert shall continue to have an annual risk assessment of the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information performed by an independent third party. The assessment shall be written and include (i) criteria for the evaluation and categorization of identified security risks or threats; (ii) criteria for the assessment of the confidentiality, integrity, and availability of Weichert's Information Systems and customer information, including the adequacy of existing controls in the context of the identified risks or threats; (iii) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks. Such reports shall be maintained by the CISO, made available for inspection by the Third-Party Assessor described in Paragraphs 6.6 through 6.8 of this Consent Order, and a copy of the report shall be produced to the Division within ten (10) days of completion for a total period of four (4) years.

n. Penetration Testing/Monitoring: Weichert shall continue to regularly test or otherwise monitor the effectiveness of safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, Information Systems connected to the Weichert Network. For Information Systems, the monitoring or testing shall continue to include continuous monitoring or periodic penetration testing and vulnerability assessments.

o. Email Filtering and Phishing Solutions: Weichert shall maintain email protection and filtering solutions for all of Weichert's email accounts, including the filtering of SPAM, phishing attacks, and other email malware attacks.

p. Employee Training: In addition to the requirements set forth in Paragraph 6.3(f) above, Weichert shall continue to conduct an initial training for all new employees no later than thirty (30) days after their employment, and on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of PI and NPI, and the risks identified by the risk assessment.

q. Data Loss/Exfiltration Prevention: Weichert shall continue to implement and maintain a data loss prevention technology, or reasonably equivalent technology, to detect and prevent unauthorized data exfiltration from the Weichert Network.

6.5 Weichert shall continue to regularly evaluate the Program, at least on an annual basis, and modify as necessary in light of the results of the requirements of Paragraph 6.4, any material changes to Weichert's operations or business arrangements, or any other circumstances that Weichert knows or has reason to know may have a material impact on the Program.

IV. *Information Security Program Assessment*

6.6 Within one hundred fifty (150) days of the Effective Date and annually for four (4) years thereafter, with respect to any business that Weichert owns, has a Controlling Interest in, manages, or controls, Weichert shall obtain and pay for an assessment of its Program pertaining to the collection, storage, maintenance, transmission, and disposal of PI and NPI from an independent Third-Party Assessor.

6.7 The Third-Party Assessor shall review this Consent Order, Security Incident Reports, and risk assessments provided by Weichert as set forth in Paragraphs 6.2 and 6.4(m). The Third-Party Assess shall prepare an annual report of findings ("Report"). The Report shall confirm Weichert has complied with the provisions of this Consent Order, and must include an assessment of Weichert's compliance with each of the requirements of this Consent Order; an assessment of Weichert's response to any Security Incidents which may have occurred each year since the

Effective Date; and documentation of the basis of the Report.

6.8 The initial Report shall be provided to the Division no later than one hundred eighty (180) days after the Effective Date, and each subsequent Report shall be provided to the New Jersey Division of Consumer Affairs (“Division”) no later than thirty (30) days after the report is completed by the Third-Party Assessor. Weichert will also provide the risk assessment, as set forth in Paragraph 6.4(m), to the New Jersey Attorney General on an annual basis during the four-year term.

6.9 Following the four-year terms specified in Paragraphs 6.4(m), 6.6, and 6.8, Weichert shall continue to conduct risk assessments and Information Security Program assessments on an annual basis for the following three (3) years, as required by the GLBA and as determined by the CISO, which are to be memorialized in written Reports. The Division reserves the right to request copies of the Reports from any Information Security Program assessments and risk assessments conducted by Weichert for three (3) years following the five-year terms specified in Paragraphs 6.4(m), 6.6, and 6.8.

6.10 Confidentiality: The Division, shall, to the extent permitted by State law, treat all documents produced pursuant to Paragraphs 6.4(m), 6.6, 6.8, and 6.9 as exempt from disclosure as applicable under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 to -13.

7. RELEASE

7.1 In consideration of the undertakings, mutual promises, and obligations provided for in this Consent Order and conditioned on Weichert making the Payment to New Jersey as described in Section 5, the Division hereby agrees to release Weichert from any and all civil claims, or consumer-related administrative claims or actions, to the extent permitted by law, which the Division could have brought prior to the Effective Date against Weichert that are related to and/or arise from the Data Breaches, including, any claims under the CFA, ITPA, and the GLBA

(“Released Claims”). Nothing contained in this paragraph shall be construed to limit the ability of the Division to enforce the obligations that Weichert, their officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Consent Order.

7.2 Notwithstanding any term of this Consent Order, any and all of the following forms of liability are specifically reserved and excluded from the Released Claims: (a) private rights of action; (b) actions to enforce this Consent Order; and (c) any claims against Weichert by any other agency or subdivision of the State except any civil claims or causes of action, or consumer-related administrative claims or actions, arising out of the Investigation as well as matters specifically addressed in this Consent Order that the Division could have brought but has released in Paragraph 7.1 above.

8. NOTICES

8.1 Unless otherwise provided, any notices or documents required to be sent pursuant to this Consent Order shall be sent to the following addresses via overnight courier and electronic mail (unless after the Effective Date, a different address is communicated in writing by the party requesting a change or designee or address):

a. For the Attorney General:

Cody I. Valdez, Deputy Attorney General,
Data Privacy and Cybersecurity Section,
New Jersey Division of Law,
124 Halsey St., 5th Floor,
P.O. Box 45029, Newark, New Jersey 07101
Cody.Valdez@law.njoag.gov.

b. For Weichert:

Anjali C. Das, Attorney at Law,
Wilson Elser Moskowitz Edelman & Dicker LLP,
55 West Monroe Street, Suite 3800,
Chicago, Illinois 60603
Anjali.Das@wilsonelser.com.

Jennifer S. Stegmaier, Attorney at Law,
Wilson Elser Moskowitz Edelman & Dicker LLP,
55 West Monroe Street, Suite 3800
Chicago, Illinois 60603
Jennifer.Stegmaier@wilsonelser.com.

9. PENALTIES FOR FAILURE TO COMPLY

9.1 The Attorney General (or designated representative) shall have the authority to enforce the provisions of this Consent Order or to seek sanctions for violations hereof or both.

9.2 Prior to filing any action to enforce the provisions of this Consent Order, the Attorney General (or designated representative) shall meet and confer with Weichert in an attempt to resolve any dispute with respect to compliance with this Consent Order. The Attorney General (or designated representative) shall notify Weichert in writing of the alleged violation of this Consent Order, and Weichert shall have thirty (30) days to respond to the notification. The Attorney General (or designated representative) shall not file any action until the thirty (30) days expires.

10. COMPLIANCE WITH ALL LAWS

10.1 Except as provided in this Consent Order, no provision herein shall be construed as:

a. Relieving Weichert of their obligations to comply with all State and federal laws, regulations, or rules as now constituted or as may hereafter be amended; granting permission to engage in any acts or practices prohibited by any such laws, regulations, or rules; or requiring Weichert to take an action that is prohibited by such laws, regulations, or rules; or

b. Limiting or expanding any right the Division may otherwise have to obtain information, documents, or testimony from Weichert pursuant to any State or federal law, regulation, or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right Weichert may otherwise have pursuant to any State or federal law, regulation, or rule, to

oppose any process employed by the Division to obtain such information, documents, or testimony.

11. GENERAL PROVISIONS

11.1 This Consent Order is entered into by the Parties as their own free and voluntary act with full knowledge and understanding of the obligations and duties imposed by this Consent Order.

11.2 This Consent Order shall be governed by, and construed and enforced in accordance with, the laws of the State of New Jersey.

11.3 The Parties have negotiated, jointly drafted, and fully reviewed the terms of this Consent Order and the rule that uncertainty or ambiguity is to be construed against the drafter shall not apply to the construction or interpretation of this Consent Order.

11.4 This Consent Order contains the entire agreement among the Parties. Except as otherwise provided herein, this Consent Order shall be modified only by a written instrument signed by or on behalf of all Parties.

11.5 Except as otherwise explicitly provided in this Consent Order, nothing herein shall be construed to limit the authority of Plaintiffs to protect the interest of the State or the people of the State, or to enforce any laws, regulations, or rules against Weichert.

11.6 If any portion of this Consent Order is held invalid or unenforceable by operation of law, the remaining terms of this Consent Order shall not be affected.

11.7 This Consent Order shall be binding upon the Parties and their successors in interest. In no event shall assignment of any right, power, or authority under this Consent Order avoid compliance with this Consent Order.

11.8 This Consent Order is entered into by the Parties for settlement purposes only. Neither the fact of nor any provision contained in this Consent Order shall constitute or be

construed as: (a) an approval, sanction, or authorization by the Attorney General, the Division, or any other governmental unit of the State of any act or practice of Weichert; or (b) an admission by Weichert that it violated the CFA, ITPA, or GLBA, or any other federal or State law, administrative rule or regulation, or an express or implied admission of any other matter of fact or law, or of any liability or wrongdoing.

11.9 This Consent Order is not intended, and shall not be deemed, to constitute evidence or precedent of any kind in any action or proceeding except in: (a) an action or proceeding by one of the Parties to enforce, rescind, or otherwise implement any or all of the terms herein; or (b) an action or proceeding involving a Released Claim (as defined in Section 7) to support a defense of res judicata, collateral estoppel, release, or any other theory of claim preclusion, issue preclusion, or similar defense.

11.10 The Parties represent and warrant that their signatories to this Consent Order have the authority to act for and bind the respective Party.

11.11 Unless otherwise prohibited by law, any signatures by the Parties required for the filing of this Consent Order may be executed in counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same Consent Order. Electronic signatures shall constitute acceptable, binding signatures for purposes of this Consent Order.

IT IS ON THE 18th DAY OF May, 2022, SO ORDERED, ADJUDGED AND DECREED.

MATTHEW J. PLATKIN

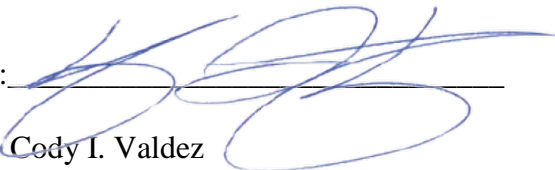
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: *Cari Fais*
CARI FAIS, ACTING DIRECTOR
DIVISION OF CONSUMER AFFAIRS

FOR THE DIVISION:

MATTHEW J. PLATKIN

ACTING ATTORNEY GENERAL OF NEW JERSEY

By:  Dated: May 17, 2022
Cody I. Valdez
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101

FOR WEICHERT CO. D/B/A WEICHERT REALTORS; MORTGAGE ACCESS CORP.
D/B/A WEICHERT FINANCIAL SERVICES; WEICHERT INSURANCE AGENCY, INC.;
TITLE CLOSING SERVICES, LLC D/B/A WEICHERT TITLE AGENCY D/B/A
DEMOCRACY TITLE AGENCY; and AFFILIATES:

By: 

Dated: May 13, 2022

Jennifer S. Stegmaier
Wilson Elser Moskowitz Edelman & Dicker LLP
55 West Monroe Street, Suite 3800
Chicago, Illinois 60603