597 F.3d 263
United States Court of Appeals,
Fifth Circuit.

UNITED STATES of America, Plaintiff–Appellee,
v.
Dimetriace Eva–Lavon JOHN,
Defendant–Appellant.

No. 08–10459. | Feb. 9, 2010.

Synopsis

Background: Defendant was convicted of conspiracy to commit access device fraud, fraud in connection with an access device and aiding and abetting, and exceeding authorized access to a protected computer, following jury trial in the United States District Court for the Northern District of Texas, Jorge A. Solis, J. Defendant appealed.

Holdings: The Court of Appeals, Owen, Circuit Judge, held that:

[1] convictions for exceeding authorized access to employer's computers did not constitute manifest miscarriage of justice;

[2] District Court was not required to hold *Daubert* hearing prior to determining admissibility of expert witness testimony concerning fingerprints;

[3] District Court's adherence to hearsay rule, in refusing to allow police officers who interrogated defendant's half-brother to testify, did not violate defendant's constitutional rights;

[4] any error that occurred when employer's vice president expressed opinion regarding what employee acting properly within scope of employment would have done in a particular situation was harmless;

[5] District Court did not clearly err in determining amount of loss for sentencing purposes;

[6] three-level reduction due to offense being partially completed applied to defendant;

[7] District Court's error in failing to grant three-level reduction affected defendant's substantial rights, as required for plain error; and

[8] such error seriously affected fairness, integrity, or public reputation of judicial proceedings, as required for plain error.

Affirmed in part, vacated in part, and remanded.

Jerry E. Smith, Circuit Judge, filed dissenting opinion.

Attorneys and Law Firms

***269** Marc Woodson Barta, Asst. U.S. Atty. (argued), Dallas, TX, for U.S.

Kevin Joel Page (argued), Fed. Pub. Def., Dallas, TX, for John.

Appeal from the United States District Court for the Northern District of Texas.

Before SMITH, OWEN and HAYNES, Circuit Judges.

Opinion

OWEN, Circuit Judge:

Dimetriace Eva–Lavon John was found guilty by a jury on all counts of a seven-count indictment arising out of her involvement in a scheme to incur fraudulent charges on accounts held by various Citigroup customers. John challenges her convictions and sentence in this appeal. We affirm the convictions but vacate her sentence and remand for further proceedings.

I

Dimetriace Eva–Lavon John was employed as an account manager at Citigroup for approximately three years. By virtue of her position, she had access to Citigroup's internal computer system and customer account information contained in it. In September 2005, John

provided Leland Riley, her half-brother, with customer account information enabling Riley and other confederates to incur fraudulent charges.

John accessed and printed information pertaining to at least seventy-six corporate customer accounts and provided it to Riley. The information was in the form of either scanned images of checks written by the account holders or printouts of computer screens containing detailed account information. Before he was apprehended, Riley and cohorts used information John had provided to incur fraudulent charges on four different accounts.

A grand jury returned a seven-count indictment against John. Count 1 charged John with conspiracy to commit access device fraud in violation of 18 U.S.C. § 371. Counts 2 through 5 charged John with fraud in connection with an access device and aiding and abetting, in violation of 18 U.S.C. §§ 1029(a)(5) and (2). Counts 6 ***270** and 7 charged John with exceeding authorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C). A jury found John guilty on all seven counts.

[. . .]

II

[1] John has raised several issues regarding her convictions. Her first contention is that the evidence was insufficient to support her convictions on Counts 6 and 7 under 18 U.S.C. § 1030(a)(2) for exceeding authorized access to Citigroup's computers. She candidly acknowledges that at trial her counsel failed to renew a motion for acquittal at the close of the evidence and that we therefore may only reverse her convictions on these counts "if there was a 'manifest miscarriage of justice,' which would occur if there is no evidence of the defendant's guilt or 'the evidence on a key element of the offense was so tenuous that a conviction would be shocking.' "[2]

Whether John's convictions on Counts 6 and 7 may be sustained depends on the proper interpretation of "exceeds authorized access" as used in § 1030(a)(2) and defined in § 1030(e)(6).

John was convicted of violating § 1030(a)(2), which provides:

> (a) Whoever—
>
> ...
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); ...
>
> shall be punished as provided in subsection (c) of this section.[3]

The term "exceeds authorized access" is defined in § 1030(e)(6): "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the ***271** computer that the accesser is not entitled so to obtain or alter...."

John argues that she was authorized to use Citigroup's computers and to view and print information regarding accounts in the course of her official duties. The evidence, she contends, reflects only that she was not permitted to use the information to which she had access to perpetrate a fraud, she could make changes to account information only in compliance with a customer's request, and she was not permitted to take material she printed regarding accounts from her office building. She asserts that her mental state or motive at the time she accessed or printed account information cannot determine whether she violated 18 U.S.C. § 1030(a)(2). Specifically, she argues that the statute does not prohibit unlawful *use* of material that she was authorized to access through authorized use of a computer. The statute only prohibits using authorized access to obtain information that she is not entitled to obtain or alter information that she is not entitled to alter, John contends.

We first note that John was not charged in Counts 6 or 7 with altering information in Citigroup's computer system. She was charged with "exceeding authorized access" and

obtaining confidential Citigroup and Home Depot customer account information.

[2] The statute at issue prohibits both accessing a computer "without authorization" and "exceed[ing] authorized access" to obtain specified information.[4] The statute does not define "authorized," or "authorization," which is used in the definition of "exceeds authorized access."[5] The question before us is whether "authorized access" or "authorization" may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system. We conclude that it may, at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.

To give but one example, an employer may "authorize" employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business. An employee would "exceed [ ] authorized access" if he or she used that access to obtain or steal information as part of a criminal scheme.

In *United States v. Phillips*, this court analyzed whether a criminal defendant had accessed university computers "without authorization" in violation of § 1030(a)(5)(A)(ii), as distinguished from "exceed[ing] authorized access," and we recognized that "[c]ourts have ... typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."[6] We applied this "intended-use analysis" to conclude that a student who used his privilege of access to a university's computer was not authorized to access parts of the system to which he had not been given a password.[7] John's situation differs from that of the student in *Phillips* because John was authorized to view and print all of the information that she accessed ***272** and that she provided to Riley. However, John's use of Citigroup's computer system to perpetrate fraud was not an intended use of that system.

John's use of Citigroup's computer system to perpetrate a fraud was also contrary to Citigroup employee policies, of which she was aware. The First Circuit has held that an employment agreement can establish the parameters of "authorized" access. In *EF Cultural Travel BV v. Explorica, Inc.*, the plaintiffs brought a civil action under the Computer Fraud and Abuse Act (CFAA)[8] seeking injunctive relief against former employees who had become competitors.[9] The former employees used their knowledge of codes that they had obtained while in their former employment to create a high-speed computer program to mine their former employer's public website for pricing information.[10] The former employees had entered into a broad confidentiality agreement with their former employers protecting proprietary information.[11] The First Circuit held "that because of the broad confidentiality agreement [the former employees'] actions 'exceed[ed] authorized access' " within the meaning of § 1030(a)(4).[12] The court reasoned, "[the former employees'] wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."[13] The court continued, "[i]f EF's allegations are proven, it will likely prove that whatever authorization [former employees] had to navigate around EF's site (even in a competitive vein), [they] exceeded that authorization by providing proprietary information and know-how to [a programmer] to create the scraper."[14]

[3] While we do not necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural Travel BV* would give rise to criminal culpability, we do agree with the First Circuit that the concept of "exceeds authorized access" may include exceeding the purposes for which access is "authorized." Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded. In other words, John's access to Citigroup's data was confined. She was not authorized to access that information for any and all purposes but for limited purposes.

In the present case, the Government demonstrated at trial that Citigroup's official policy, which was reiterated in training programs that John attended, prohibited misuse of the company's internal computer systems and confidential customer information. Despite being aware of these policies, John accessed account information for individuals whose accounts she did not manage, removed this highly sensitive and confidential information from Citigroup premises, and ultimately used this information to perpetrate fraud on Citigroup and its customers.

We recognize that the Ninth Circuit may have a different view of how "exceeds authorized access" should be construed. In *LVRC Holdings LLC v. Brekka*, a civil

proceeding, the Ninth Circuit construed ***273** 18 U.S.C. § 1030(a)(2) to mean that "a person who 'intentionally accesses a computer without authorization,' §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who 'exceeds authorized access,' *id.*, has permission to access the computer, but accesses information on the computer that the person is not entitled to access."[15] That court stated that "[t]he definition of the term 'exceeds authorized access' from § 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer."[16] In *Brekka* it was alleged that an employee e-mailed to his and his wife's personal computers proprietary documents to which his employer had given him access with the intention of using the information to compete with his employer once he resigned.[17] The court rejected the argument that one who is authorized to obtain information stored in a computer exceeds authorized access within the meaning of 18 U.S.C. § 1030(a)(2) "if the defendant breaches a state law duty of loyalty to an employer" in accessing and using that information[18] "to further his own competing business."[19]

The Ninth Circuit's reasoning in *Brekka* was influenced by its recognition that "[f]irst, and most important, § 1030 is primarily a criminal statute, and §§ 1030(a)(2) and (4) create criminal liability for violators of the statute."[20] The court explained its view that, "[a]lthough this case arises in a civil context, our interpretation of [the statute] is equally applicable in the criminal context," and that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity."[21] The Ninth Circuit explained that "[i]f the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner."[22]

There are no such concerns in the present case. An authorized computer user "has reason to know" that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme. Moreover, the Ninth Circuit's reasoning at least implies that when an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be "proper" to conclude that such conduct "exceeds authorized access" within the meaning of § 1030(a)(2).

[. . .]

We AFFIRM John's convictions. For the reasons considered above, we VACATE John's sentence and REMAND for further proceedings.

JERRY E. SMITH, Circuit Judge, dissenting:

[. . .]

Because that did not happen here, I respectfully dissent.

Footnotes

1 U.S. SENTENCING GUIDELINES MANUAL § 2X1.1(a) (2007).

2 *United States v. Villasenor*, 236 F.3d 220, 222 (5th Cir.2000) (quoting *United States v. McCarty*, 36 F.3d 1349, 1358 (5th Cir.1994) (internal quotations omitted)).

3 18 U.S.C. § 1030(a)(2)(A).

4 *Id.* § 1030(a)(2).

5 *Id.* § 1030(e)(6); *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir.2009); *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir.2007).

6 *Phillips*, 477 F.3d at 219.

7 *Id.* at 220–21.

8 18 U.S.C. § 1030.

9 274 F.3d 577, 578–79 (1st Cir.2001).

10 *Id.* at 579.

11 *Id.* at 581, 583.

12 *Id.* at 581.

13 *Id.* at 583.

14 *Id.*

15 581 F.3d 1127, 1133 (9th Cir.2009).

16 *Id.* at 1135.

17 *Id.* at 1134.

18 *Id.* at 1135 n. 7.

19 *Id.* at 1134.

20 *Id.*

21 *Id.*

22 *Id.* at 1135.

23 *United States v. Hicks*, 389 F.3d 514, 524 (5th Cir.2004) (citing *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999)).

24 *United States v. Pompa*, 434 F.3d 800, 805 (5th Cir.2005).

25 FED.R.EVID. 702.

26 *Moore v. Ashland Chem. Inc.*, 151 F.3d 269, 275 (5th Cir.1998) (en banc).

27 *Hicks*, 389 F.3d at 525 (citing *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 593–94, 113 S.Ct. 2786, 125 L.Ed.2d 469

(1993)).

28 *Id.*

29 *Id.; see also Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 150–53, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999).

30 *See, e.g., United States v. Mitchell*, 365 F.3d 215, 246 (3d Cir.2004) (holding that a district court may dispense with a *Daubert* hearing entirely if no novel challenge is raised to the admissibility of latent fingerprint identification evidence); *United States v. Crisp*, 324 F.3d 261, 268 (4th Cir.2003) (stating, in the context of fingerprint evidence, that "[u]nder *Daubert*, a trial judge need not expend scarce judicial resources reexamining a familiar form of expertise every time opinion evidence is offered").

31 *United States v. Havvard*, 260 F.3d 597, 601 (7th Cir.2001).

32 *See United States v. Abreu*, 406 F.3d 1304, 1307 (11th Cir.2005) (holding that fingerprint evidence satisfies *Daubert*); *Crisp*, 324 F.3d at 267–70 (same); *United States v. Collins*, 340 F.3d 672, 682–83 (8th Cir.2003) (same); *Havvard*, 260 F.3d at 601 (same); *United States v. Sherwood*, 98 F.3d 402, 408 (9th Cir.1996) (same).

33 *Crisp*, 324 F.3d at 266.

34 *Havvard*, 260 F.3d at 601.

35 *See, e.g., id.; Mitchell*, 365 F.3d at 240.

36 *See Mitchell*, 365 F.3d at 236 (describing the FBI "sliding scale" standard, which considers both the quality and quantity of matching points); *Crisp*, 324 F.3d at 269 (noting that "while different agencies may require different degrees of correlation before permitting a positive identification, fingerprint analysts are held to a consistent 'points and characteristics' approach to identification"); *Havvard*, 260 F.3d at 599 (stating that the expert testified that the "unique nature of fingerprints is counterintuitive to the establishment of [a numerical] standard and that through experience each examiner develops a comfort level for deciding how much of a fragmentary print is necessary to permit a comparison").

37 *Mitchell*, 365 F.3d at 237–38, 241, 244–46; *see also United States v. Mahone*, 453 F.3d 68, 72 (1st Cir.2006) (holding that in light of the fact that the adversarial system is the proper venue for testing shaky, but admissible, evidence, the argument that the lack of a set number of clues required for a match invalidates fingerprint evidence must be rejected).

38 *Crisp*, 324 F.3d at 269; *Havvard*, 260 F.3d at 599.

39 *United States v. George*, 363 F.3d 666, 673 (7th Cir.2004) (noting that having found fingerprint analysis in general to be reliable, any issues regarding the match in question are best resolved by the fact finder).

40 *See Havvard*, 260 F.3d at 599.

41 *See United States v. Wells*, 525 F.2d 974, 976 (5th Cir.1976) ("There was an exception taken to the court's ruling sustaining the Government's [hearsay] objection, but no offer of proof. Inasmuch as no suggestion was made at the time that the evidence sought would fall within some exception to the hearsay rule, appellants cannot properly contend now that it was error to sustain Government's objections to the questions in issue."); *see also Elizarraras v. Bank of El Paso*, 631 F.2d 366, 374 n. 24 (5th Cir.1980) (noting that because there was no proffer, the exclusion of testimony on hearsay grounds would be impossible to review).

42 *Holmes v. South Carolina*, 547 U.S. 319, 324, 126 S.Ct. 1727, 164 L.Ed.2d 503 (2006) (internal quotation marks and alteration omitted). Examples of rules that the Court has found "arbitrary or disproportionate" include (1) a rule precluding a person who had been charged as a participant in a crime from testifying for the defense—but not the prosecution—of another alleged participant,

unless the witness had been acquitted; (2) a "voucher rule" that barred parties from impeaching their own witnesses where alternative avenues for impeachment were foreclosed by the hearsay rule; and (3) a rule applying a per se prohibition on any hypnotically refreshed testimony. *Id.* at 325–27, 126 S.Ct. 1727.

43 *Chambers v. Mississippi*, 410 U.S. 284, 302, 93 S.Ct. 1038, 35 L.Ed.2d 297 (1973).

44 *Id.*

45 *See id.* at 302–03, 93 S.Ct. 1038 (stating that the decision did not announce any new principles of constitutional law but that the holding was simply that "under the facts and circumstances of this case the rulings of the trial court deprived Chambers of a fair trial").

46 *Id.* at 300–01, 93 S.Ct. 1038.

47 *Id.* at 300, 93 S.Ct. 1038.

48 *Id.* at 300–01, 93 S.Ct. 1038.

49 *Id.* at 296–98, 93 S.Ct. 1038.

50 *United States v. Saldana*, 427 F.3d 298, 306 (5th Cir.2005).

51 *Texas A&M Research Found. v. Magna Transp., Inc.*, 338 F.3d 394, 403 (5th Cir.2003) (alteration in original) (internal quotation marks omitted).

52 *See id.; see also DIJO, Inc. v. Hilton Hotels Corp.*, 351 F.3d 679, 685 (5th Cir.2003) (stating that business owners or officers may testify as to their opinion based on "particularized knowledge derived from their position" (emphasis omitted)).

53 *See Washington v. Shop–Vac Corp.*, 8 F.3d 296, 300 (5th Cir.1993) (holding that the district court did not abuse its discretion by excluding a witness's testimony regarding "what he would have done" in a particular situation because that opinion was speculative and not based on personal knowledge).

54 U.S.S.G. § 2B1.1(b)(1) (2007).

55 *Id.*

56 § 2B1.1 cmt. background (2007).

57 § 2B1.1 cmt. n. 3(A).

58 *United States v. Henderson*, 19 F.3d 917, 928 (5th Cir.1994); *see also United States v. Sanders*, 343 F.3d 511, 527 (5th Cir.2003) (stating that the Government must "prove by a preponderance of the evidence that the defendant had the subjective intent to cause the loss that is used to calculate his offense level").

59 *United States v. Brown*, 7 F.3d 1155, 1159 (5th Cir.1993).

60 *United States v. Ismoila*, 100 F.3d 380, 396 (5th Cir.1996).

61 § 2B1.1 cmt. n. 3(C).

62 *United States v. Sowels,* 998 F.2d 249, 251 (5th Cir.1993).

63 *United States v. Krenning,* 93 F.3d 1257, 1269 (5th Cir.1996).

64 *See, e.g., Ismoila,* 100 F.3d at 396 ("Available credit is ... one way of determining intended loss.").

65 6 F.3d 1095, 1101 (5th Cir.1993).

66 *Id.*

67 *Id.*

68 *Sowels,* 998 F.2d at 250–51; *see id.* (noting in particular that "Sowels's method of operation, which included selling or giving away some of the credit cards to others, 'increased the likelihood that the credit cards could have been charged to the maximum credit limit' " and that Sowels previously charged high balances on stolen credit cards in a short period).

69 *Id.* at 252.

70 *Id.* at 251.

71 *See, e.g., id.* (approving the inclusion of aggregate credit limits for yet-to-be-used cards, noting that in such a case the defendant "put[s] his victims at risk for the aggregate amount of the unused balances"); *see also United States v. Wimbish,* 980 F.2d 312, 316 (5th Cir.1992) (concluding that the court could consider the face amount of forged checks in calculating intended loss, even though the defendant's plan was to receive only a portion of the check value because "[h]is actions and his conscious indifference put his victims at risk for the entire loss, regardless of how much he actually obtained"), *abrogated on other grounds by Stinson v. United States,* 508 U.S. 36, 113 S.Ct. 1913, 123 L.Ed.2d 598 (1993).

72 *See United States v. Oates,* 122 F.3d 222, 226 (5th Cir.1997) (holding that the full amount of a not-yet-presented fraudulent check was the intended loss because the defendant gained immediate access to the funds by indorsing the instrument).

73 *See United States v. Ismoila,* 100 F.3d 380, 396 (5th Cir.1996).

74 *Id.*

75 *United States v. Brown,* 7 F.3d 1155, 1159 (5th Cir.1993).

76 *See Sowels,* 998 F.2d at 251.

77 U.S.S.G. § 2B1.1 cmt. 17.

78 *Id.*

79 *Id.* § 2X1.1 cmt. 4.

80 *Id.* cmt. Background.

81 *See United States v. Garza–Lopez,* 410 F.3d 268, 272 (5th Cir.2005).

82 *United States v. Price,* 516 F.3d 285, 287 (5th Cir.2008).

83 *United States v. Rothman,* 914 F.2d 708, 709 (5th Cir.1990).

84 18 U.S.C. § 1029(a)(5).

85 179 F.3d 303, 308–09 (5th Cir.1999).

86 *Id.* at 308.

87 *Id.* at 312.

88 18 U.S.C. § 1029(a)(5) ("Whoever—knowingly and with intent to defraud effects transactions with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1–year period the aggregate of which is equal to or greater than $1,000....").

89 U.S.S.G. § 2X1.1 cmt. 4.

90 *See also United States v. Khawaja,* 118 F.3d 1454, 1459 (4th Cir.1997); *United States v. Mancuso,* 42 F.3d 836, 849–50 (4th Cir.1994); *United States v. Sprecher,* 988 F.2d 318, 321 (2d Cir.1993); *but see United States v. Knox,* 112 F.3d 802, 813 (5th Cir.1997), *vacated in part on other grounds by United States v. Knox,* 120 F.3d 42 (5th Cir.1997); *United States v. Mullen,* 986 F.2d 503 (8th Cir.1993) (unpublished table decision).

91 *See Puckett v. United States,* —— U.S. ——, 129 S.Ct. 1423, 1429, 173 L.Ed.2d 266 (2009) (explaining that plain error has four prongs: (1) there was an error or defect, a "deviation from a legal rule—that has not been intentionally relinquished or abandoned"; (2) "the legal error must be clear or obvious, rather than subject to reasonable dispute"; (3) the error affected the defendant's substantial rights, "which in the ordinary case means he must demonstrate that it 'affected the outcome of the district court proceedings' "; and (4) when these three elements are present, a court may exercise its discretion to correct the error, although this discretion "ought to be exercised only if the error 'seriously affect[s] the fairness, integrity, or public reputation of judicial proceedings' " (quoting *United States v. Olano,* 507 U.S. 725, 732–36, 113 S.Ct. 1770, 123 L.Ed.2d 508 (1993))).

92 *Id.*

93 *Id.* at 1433 n. 4, 129 S.Ct. 1423.

94 *United States v. Price,* 516 F.3d 285, 289 (5th Cir.2008) (quoting *United States v. Gonzales,* 484 F.3d 712, 716 (5th Cir.2007) (internal quotation marks omitted)).

95 The offense level for John based on a loss amount of $78,750 would be 22, which is less than 27, the offense level based on the loss amount of $1,451,865 less the 3–level reduction. Accordingly, the offense level of 27 would apply under the Guidelines, assuming no other error in the calculation of the advisory Guidelines range.

96 *See, e. g., United States v. Villegas,* 404 F.3d 355, 364–65 (5th Cir.2005) (concluding that Villegas's substantial rights were affected when the proper application of the Guidelines resulted in an advisory sentencing range of 10–16 months, as compared to a 21–27–month range calculated by the district court); *United States v. Insaulgarat,* 378 F.3d 456, 468 n. 17 (5th Cir.2004); *United*

States v. Gracia–Cantu, 302 F.3d 308, 313 (5th Cir.2002); *United States v. Waskom,* 179 F.3d 303, 312 (5th Cir.1999); *see also Price,* 516 F.3d at 289 (determining that a sentencing error affected Price's substantial rights even though the Guidelines sentencing range calculated by the district court and the correct sentencing range overlapped because the low end of the correct sentencing range, 92 months of imprisonment, was substantially (18 months) lower than Price's actual sentence of 110 months of imprisonment).

97 *See Puckett,* 129 S.Ct. at 1432–33 ("The defendant whose plea agreement has been broken by the Government will not always be able to show prejudice, either because he obtained the benefits contemplated by the deal anyway ... or because he likely would not have obtained those benefits in any event....").

98 *Id.* at 1429.

99 *Id.* (quoting *United States v. Dominguez Benitez,* 542 U.S. 74, 83 n. 9, 124 S.Ct. 2333, 159 L.Ed.2d 157 (2004)).

100 *See, e.g., Villegas,* 404 F.3d at 365 (concluding that "because the district court's error clearly affected Villegas's sentence, we also find that the error seriously affected the fairness, integrity, or public reputation of judicial proceedings"); *see also United States v. Ellis,* 564 F.3d 370, 378 (5th Cir.2009) (recognizing that this court's sentencing precedent "has been generous with remand, often finding that errors leading to substantial increases in sentences, even those errors not raised until appeal and thus subject to plain error review, merited remand, although we are not convinced that the case law on this point is settled or as categorical as language in some cases might make it seem"), *cert. denied,* —— U.S. ——, 130 S.Ct. 371, 175 L.Ed.2d 124 (2009); *id.* at 378 n. 44 (collecting cases "indicat[ing] some variation in treatment of plain error review, but with a generally permissive approach to the third and fourth prongs, and especially where a significantly different Guidelines range was erroneously advised"); *Price,* 516 F.3d at 290.

101 *See, e.g., Price,* 516 F.3d at 290.

102 *Puckett,* 129 S.Ct. at 1433 (quoting *United States v. Young,* 470 U.S. 1, 16 n. 14, 105 S.Ct. 1038, 84 L.Ed.2d 1 (1985)).

103 *Gall v. United States,* 552 U.S. 38, 49, 128 S.Ct. 586, 169 L.Ed.2d 445 (2007).

104 *Id.* at 50, 128 S.Ct. 586.

105 *Id.; see also Rita v. United States,* 551 U.S. 338, 357, 127 S.Ct. 2456, 168 L.Ed.2d 203 (2007).

106 *See Rita,* 551 U.S. at 357–58, 127 S.Ct. 2456 ("By articulating reasons, even if brief, the sentencing judge not only assures reviewing courts (and the public) that the sentencing process is a reasoned process but also helps that process evolve .... [A] reasoned sentencing judgment, resting upon an effort to filter the Guidelines' general advice through § 3553(a)'s list of factors, can provide relevant information to both the court of appeals and ultimately the Sentencing Commission.").

107 *United States v. Ellis,* 564 F.3d 370, 378 (5th Cir.2009), *cert. denied,* —— U.S. ——, 130 S.Ct. 371, 175 L.Ed.2d 124 (2009); *see, e.g., United States v. Villegas,* 404 F.3d 355, 365 (5th Cir.2005) (concluding that "because the district court's error clearly affected Villegas's sentence" by increasing Villegas's sentencing range from 10–16 months to 21–27 months, "the error seriously affected the fairness, integrity, or public reputation of judicial proceedings"); *see also Ellis,* 564 F.3d at 378 n. 44 (collecting cases "indicat[ing] some variation in treatment of plain error review, but with a generally permissive approach to the third and fourth prongs, and especially where a significantly different Guidelines range was erroneously advised").

108 *Ellis,* 564 F.3d at 378.

109 *See United States v. Meacham,* 567 F.3d 1184, 1190 (10th Cir.2009) ("A review of federal appellate decisions considering whether to correct unobjected-to sentencing errors reveals that the key concern has been whether correct application of the sentencing laws would likely significantly reduce the length of the sentence. When circuit courts have concluded that it would, they have not

hesitated to exercise their discretion to correct the error."); *see also In re Sealed Case*, 573 F.3d 844, 853 (D.C.Cir.2009) ("We have repeatedly opted to correct plain sentencing errors, that, if left uncorrected, would result in a defendant serving a longer sentence."); *id.* ("We cannot say that keeping defendant in prison longer for improper reasons would leave the fairness, integrity, and public reputation of judicial proceedings unscathed."); *United States v. Avila*, 557 F.3d 809, 822 n. 23 (7th Cir.2009) (vacating 396–month sentence that was above a range of 262–327 months after correction of at least one of the sentencing errors committed by the district court).

110 *See United States v. Garrett*, 528 F.3d 525, 530 (7th Cir.2008) (alterations omitted) (concluding that sentencing error seriously affects the integrity of judicial proceedings whenever the miscalculation leads to a higher Guidelines range); *see also Avila*, 557 F.3d at 822 ("A sentence based on an incorrect Guideline range constitutes an error affecting substantial rights and can thus constitute plain error, which requires us to remand unless we have reason to believe that the error did not affect the district court's selection of a particular sentence.").

111 587 F.3d 706, 713 (5th Cir.2009).

112 *Id.* at 713–14.

113 516 F.3d 285, 289–90 (5th Cir.2008).

114 *See* FED.R.CRIM.P. 52(b); *Puckett v. United States*, ––U.S. ––––, 129 S.Ct. 1423, 1429, 173 L.Ed.2d 266 (2009); *United States v. Olano*, 507 U.S. 725, 732–37, 113 S.Ct. 1770, 123 L.Ed.2d 508 (1993).

115 U.S.S.G. § 2B1.1(b)(14)(A)(i) (2007).

116 § 2B1.1 cmt. n. 13(A).